PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-036015
(43)Date of publication of application : 02.02.2000

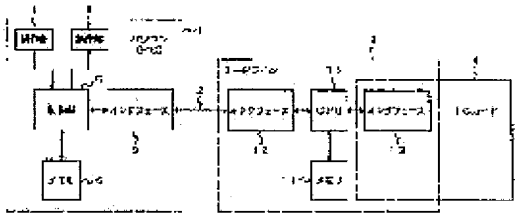
(51)Int.Cl. G06K 17/00
G06K 19/07
G06K 19/073
G09C 1/00
H04L 9/36

(21)Application number : 10-203399
(22)Date of filing : 17.07.1998

(71)Applicant : TOSHIBA CORP
(72)Inventor : NISHIOKA MITSURU

(54) IC CARD PROCESSOR, IC CARD, IC CARD PROCESSING SYSTEM AND IC CARD PROCESSING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent the leak of information concerning an issuing command and to attain improvement in the security of an IC card concerning issuing processing by hiding the telegraphic message of the issuing command to an issuing object card with a means such as enciphering.
SOLUTION: A control part 5 has an enciphering function for enciphering the telegraphic message of a command while using a production number (card peculiar information) supplied from an IC card 4 as a cryptographic key. At the time of card production, all the IC cards 4 have the same decoding logic and decoding key and on the side of a personal computer(PC) 1 for transmitting the telegraphic message of the command to the IC card 4, the correspondent encoding logic and cryptographic key are provided as well. Namely, in primary issuing processing, the same decoding logic (program) and key (decoding key) are used for all the IC cards 4 in order to create a file common for each system. In this case, the telegraphic message of the enciphered command gets equal for all the IC cards 4 but a 'command' in naked state can be hidden at least.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－36015
（P2000－36015A）
(43)公開日　平成12年２月２日(2000.2.2)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｂ	５Ｂ０３５
			Ｄ	５Ｂ０５８
19/07		Ｇ０９Ｃ　1/00	６６０Ａ	５Ｋ０１３
19/073		Ｇ０６Ｋ　19/00	Ｎ	
Ｇ０９Ｃ　1/00	６６０		Ｐ	

審査請求　未請求　請求項の数17　ＯＬ　（全 33 頁）　最終頁に続く

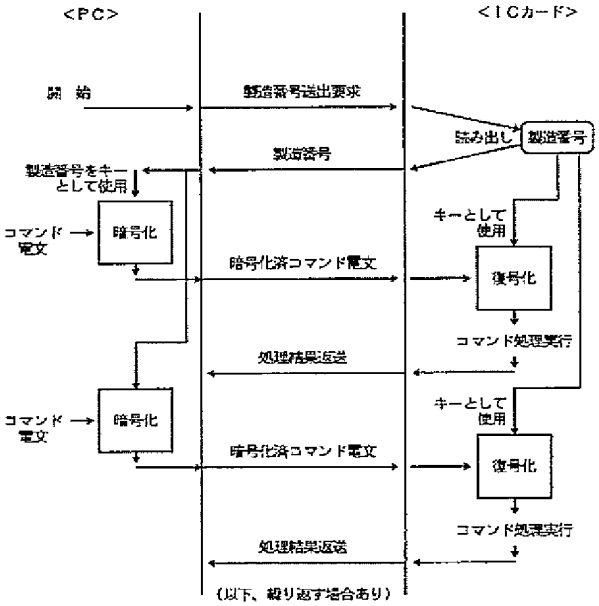
(21)出願番号　特願平10－203399
(22)出願日　平成10年７月17日(1998.7.17)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　西岡　満
神奈川県川崎市幸区柳町70番地　東芝ソシオエンジニアリング株式会社内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5B035 AA13 BB09 CA38
5B058 CA01 KA35 YA20
5K013 BA02 CA01 EA00 EA06 FA03

(54)【発明の名称】　ＩＣカード処理装置とＩＣカードとＩＣカード処理システムとＩＣカード処理方法

(57)【要約】
【課題】　この発明は、発行対象のＩＣカードに対する発行コマンド電文を暗号化等の手段により隠蔽することで、未発行のカードを入手して不正にカードを作成しようとする行為に不可欠の発行コマンドに関する情報の漏洩が防止でき、発行処理に関するＩＣカードのセキュリティを向上させることができるできる。
【解決手段】　この発明は、発行対象のＩＣカードに対する発行コマンド電文を暗号化等の手段により隠蔽するようにしたものである。



1

【特許請求の範囲】

【請求項１】　ＩＣカードへ送信するコマンド電文を生成する生成手段と、
ＩＣカードに対してカード固有番号の出力要求を上記ＩＣカードへ送信する第１の送信手段と、
この第１の送信手段に応答して得られるＩＣカードのカード固有番号を暗号キーとして上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、
この暗号化手段により暗号化されたコマンド電文を上記ＩＣカードへ送信する第２の送信手段と、
この第２の送信手段に応答して得られる処理結果に応じて処理を終了する終了手段と、
を具備したことを特徴とするＩＣカード処理装置。

【請求項２】　カード固有番号を記憶している記憶手段と、
外部装置からのカード固有番号の出力要求に応答して上記記憶手段から読出したカード固有番号を上記外部装置へ送信する第１の送信手段と、
この第１の送信手段に応答して得られる暗号化されたコマンド電文を上記記憶手段から読出したカード固有番号を復号キーとして復号化する復号化手段と、
この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段と、
この処理手段による処理結果を上記外部装置へ送信する第２の送信手段と、
を具備したことを特徴とするＩＣカード。

【請求項３】　ＩＣカード処理装置とＩＣカードとからなるＩＣカード処理システムにおいて、
上記ＩＣカード処理装置が、
ＩＣカードへ送信するコマンド電文を生成する生成手段と、
ＩＣカードに対してカード固有番号の出力要求を上記ＩＣカードへ送信する第１の送信手段と、
この第１の送信手段に応答して得られるＩＣカードのカード固有番号を暗号キーとして上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、
この暗号化手段により暗号化されたコマンド電文を上記ＩＣカードへ送信する第２の送信手段とからなり、
上記ＩＣカードが、
カード固有番号を記憶している記憶手段と、
上記ＩＣカード処理装置からのカード固有番号の出力要求に応答して上記記憶手段から読出したカード固有番号を上記ＩＣカード処理装置へ送信する第３の送信手段と、
この第３の送信手段に応答して得られる暗号化されたコマンド電文を上記記憶手段から読出したカード固有番号を復号キーとして復号化する復号化手段と、
この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる、
ことを特徴とするＩＣカード処理システム。

2

【請求項４】　ＩＣカード処理装置とＩＣカードとからなるＩＣカード処理システムにおいて、
上記ＩＣカード処理装置が、
ＩＣカードへ送信するコマンド電文を生成する生成手段と、
ＩＣカードに対してカード固有番号の出力要求を上記ＩＣカードへ送信する第１の送信手段と、
この第１の送信手段に応答して得られるＩＣカードのカード固有番号を暗号キーとして上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、
この暗号化手段により暗号化されたコマンド電文を上記ＩＣカードへ送信する第２の送信手段と、
この第２の送信手段に応答して得られる処理結果が供給された際に、上記生成手段により生成されたコマンド電文の送信を行うか終了するかを判断する判断手段と、
この判断手段によりコマンド電文の送信を判断した際に、上記ＩＣカードのカード固有番号を暗号キーとして上記生成手段により生成されたコマンド電文を上記暗号化手段により暗号化し、上記第２の送信手段により暗号化されたコマンド電文を上記ＩＣカードへ送信する第１の処理手段とからなり、
上記ＩＣカードが、
カード固有番号を記憶している記憶手段と、
上記ＩＣカード処理装置からのカード固有番号の出力要求に応答して上記記憶手段から読出したカード固有番号を上記ＩＣカード処理装置へ送信する第３の送信手段と、
この第３の送信手段に応答して得られる暗号化されたコマンド電文を上記記憶手段から読出したカード固有番号を復号キーとして復号化する復号化手段と、
この復号化手段により復号化されたコマンド電文に基づいた処理を行う第２の処理手段と、
この第２の処理手段による処理結果を上記ＩＣカード処理装置へ送信する第４の送信手段とからなる、
ことを特徴とするＩＣカード処理システム。

【請求項５】　ＩＣカード処理装置とＩＣカードとからなるＩＣカード処理システムにおいて、
上記ＩＣカード処理装置が、
ＩＣカードへ送信するコマンド電文を生成する第１の生成手段と、
ＩＣカードに対して乱数の出力要求を上記ＩＣカードへ送信する第１の送信手段と、
この第１の送信手段に応答して得られるＩＣカードからの乱数を暗号キーとして上記第１の生成手段により生成されたコマンド電文を暗号化する暗号化手段と、
この暗号化手段により暗号化されたコマンド電文を上記ＩＣカードへ送信する第２の送信手段とからなり、
上記ＩＣカードが、
カード固有番号を記憶している記憶手段と、
この記憶手段から読出したカード固有番号に基づく乱数

を生成する第２の生成手段と、
上記ＩＣカード処理装置からの乱数の出力要求に応答して上記第２の生成手段により生成された乱数を上記ＩＣカード処理装置へ送信する第３の送信手段と、
この第３の送信手段に応答して得られる暗号化されたコマンド電文を上記第２の生成手段により生成された乱数を復号キーとして復号化する復号化手段と、
この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる、
ことを特徴とするＩＣカード処理システム。
【請求項６】　ＩＣカード処理装置とＩＣカードとからなるＩＣカード処理システムにおいて、
上記ＩＣカード処理装置が、
前回の乱数を記憶する記憶手段と、
この記憶手段により読出した前回の乱数に基づく乱数を生成する第１の生成手段と、
ＩＣカードへ送信するコマンド電文を生成する第２の生成手段と、
上記第１の生成手段により生成された乱数を上記ＩＣカードへ送信する第１の送信手段と、
この第１の送信手段に応答して得られるＩＣカードからの処理準備開始応答が供給された際に、上記第１の生成手段により生成された乱数を暗号キーとして上記第２の生成手段により生成されたコマンド電文を暗号化する暗号化手段と、
この暗号化手段により暗号化されたコマンド電文を上記ＩＣカードへ送信する第２の送信手段と、
この第２の送信手段に応答して得られるＩＣカードからの応答が供給された際に、上記第１の生成手段により生成された乱数を暗号キーとして上記第２の生成手段により生成されたコマンド電文を上記暗号化手段で暗号化し、この暗号化されたコマンド電文を上記ＩＣカードへ上記第２の送信手段で送信する第１の処理手段とからなり、
上記ＩＣカードが、
上記ＩＣカード処理装置からの乱数に基づいて、処理準備開始応答を上記ＩＣカード処理装置へ送信する上記第３の送信手段と、
上記ＩＣカード処理装置からの乱数に基づいて、上記第３の送信手段に応答して得られる暗号化されたコマンド電文を復号化する復号化手段と、
この復号化手段により復号化されたコマンド電文に基づいた処理を行う第２の処理手段と、
この第２の処理手段による処理結果を上記ＩＣカード処理装置へ送信する第４の送信手段と、
この第４の送信手段に応答して得られる暗号化されたコマンド電文を、上記復号化手段で上記ＩＣカード処理装置からの乱数に基づいて復号化し、この復号化されたコマンド電文に基づいた処理を上記第２の処理手段で行う第３の処理手段とからなる、
ことを特徴とするＩＣカード処理システム。
【請求項７】　ＩＣカード処理装置とＩＣカードとキーカードとからなるＩＣカード処理システムにおいて、
上記キーカードが、
上記ＩＣカード処理装置から与えられる前回処理に使用された乱数を記憶する第１の記憶手段と、
認証データとを記憶する第２の記憶手段と、
上記ＩＣカード処理装置からの認証データと上記第２の記憶手段に記憶されている認証データとが一致した際に、上記第１の記憶手段に記憶されている前回の乱数を上記ＩＣカード処理装置へ送信する第１の送信手段とからなり、
上記ＩＣカード処理装置が、
上記キーカードへ認証データを送信する第２の送信手段と、
この第２の送信手段に応答して上記キーカードから得られる前回の乱数に基づく乱数を生成する第１の生成手段と、
この第１の生成手段で生成された乱数を上記キーカードへ送信する第３の送信手段と、
ＩＣカードへ送信するコマンド電文を生成する第２の生成手段と、
上記第１の生成手段により生成された乱数を上記ＩＣカードへ送信する第４の送信手段と、
この第４の送信手段に応答して得られるＩＣカードからの処理準備開始応答が供給された際に、上記第１の生成手段により生成された乱数を暗号キーとして上記第２の生成手段により生成されたコマンド電文を暗号化する暗号化手段と、
この暗号化手段により暗号化されたコマンド電文を上記ＩＣカードへ送信する第５の送信手段と、
この第５の送信手段に応答して得られるＩＣカードからの応答が供給された際に、上記第１の生成手段により生成された乱数を暗号キーとして上記第２の生成手段により生成されたコマンド電文を上記暗号化手段で暗号化し、この暗号化されたコマンド電文を上記ＩＣカードへ上記第５の送信手段で送信する第１の処理手段とからなり、
上記ＩＣカードが、
上記ＩＣカード処理装置からの乱数に基づいて、処理準備開始応答を上記ＩＣカード処理装置へ送信する上記第６の送信手段と、
上記ＩＣカード処理装置からの乱数に基づいて、上記第６の送信手段に応答して得られる暗号化されたコマンド電文を復号化する復号化手段と、
この復号化手段により復号化されたコマンド電文に基づいた処理を行う第２の処理手段と、
この第２の処理手段による処理結果を上記ＩＣカード処理装置へ送信する第７の送信手段と、
この第７の送信手段に応答して得られる暗号化されたコ

マンド電文を、上記復号化手段で上記ＩＣカード処理装置からの乱数に基づいて復号化し、この復号化されたコマンド電文に基づいた処理を上記第２の処理手段で行う第３の処理手段とからなる、
ことを特徴とするＩＣカード処理システム。
【請求項８】　ＩＣカード処理装置とＩＣカードとキーカードとからなるＩＣカード処理システムにおいて、
上記キーカードが、
指定コマンド番号が付与されている種々のコマンド形式と実行パラメータに応じたコマンドを記憶する第１の記憶手段と、
上記ＩＣカード処理装置からの指定コマンド番号と実行パラメータに対応するコマンドを上記第１の記憶手段から読出し、この読出したコマンドを上記ＩＣカード処理装置からの暗号キーに基づいて暗号化する暗号化手段と、
この暗号化手段により暗号化した暗号化済みコマンドを上記ＩＣカード処理装置へ送信する第１の送信手段とからなり、
上記ＩＣカード処理装置が、
上記ＩＣカードに対してカード固有番号の出力要求を送信する第１の送信手段と、
上記キーカードへ指定コマンド番号と実行パラメータと上記第１の送信手段に応答して得られるＩＣカードのカード固有番号としての暗号キーを送信する第２の送信手段と、
この第２の送信手段に応答して上記キーカードから得られる暗号化済みコマンドを上記ＩＣカードへ送信する第３の送信手段とからなり、
上記ＩＣカードが、
カード固有番号を記憶している第２の記憶手段と、
上記ＩＣカード処理装置からのカード固有番号の出力要求に応答して上記第２の記憶手段から読出したカード固有番号を上記ＩＣカード処理装置へ送信する第３の送信手段と、
この第３の送信手段に応答して得られる暗号化されたコマンド電文を上記第２の記憶手段から読出したカード固有番号を復号キーとして復号化する復号化手段と、
この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる、
ことを特徴とするＩＣカード処理システム。
【請求項９】　ＩＣカード処理装置とＩＣカードとキーカードとからなるＩＣカード処理システムにおいて、
上記キーカードが、
指定コマンド番号が付与されている種々のコマンド形式と実行パラメータに応じたコマンドと、指定キー番号に対応する種々の暗号化キーを記憶する第１の記憶手段と、
上記ＩＣカード処理装置からの指定コマンド番号と実行パラメータに対応するコマンドを上記第１の記憶手段から読出し、上記ＩＣカード処理装置からの指定キー番号に対応する暗号化キーを読出し、この読出したコマンドを読出した暗号化キーに基づいて暗号化する暗号化手段と、
この暗号化手段により暗号化した暗号化済みコマンドを上記ＩＣカード処理装置へ送信する第１の送信手段とからなり、
上記ＩＣカード処理装置が、
上記キーカードへ指定コマンド番号と実行パラメータと指定キー番号とを送信する第１の送信手段と、
この第１の送信手段に応答して上記キーカードから得られる暗号化済みコマンドを上記ＩＣカードへ送信する第３の送信手段とからなり、
上記ＩＣカードが、
暗号化キーを記憶している第２の記憶手段と、
上記暗号化キーを上記第２の記憶手段により読出し、この読出した暗号化キーに基づいて上記ＩＣカード処理装置からの暗号化されたコマンド電文を復号化する復号化手段と、
この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる、
ことを特徴とするＩＣカード処理システム。
【請求項１０】　ＩＣカード処理装置とＩＣカードとキーカードとからなるＩＣカード処理システムにおいて、
上記キーカードが、
指定コマンド番号が付与されている種々のコマンド形式と実行パラメータに応じたコマンドと、指定キー番号に対応する種々の暗号化キーを記憶する第１の記憶手段と、
上記ＩＣカード処理装置からの指定コマンド番号と実行パラメータに対応するコマンドを上記第１の記憶手段から読出し、上記ＩＣカード処理装置からの指定キー番号に対応する暗号化キーを読出し、この読出したコマンドを読出した暗号化キーに基づいて暗号化する暗号化手段と、
この暗号化手段により暗号化した暗号化済みコマンドを上記ＩＣカード処理装置へ送信する第１の送信手段とからなり、
上記ＩＣカード処理装置が、
上記ＩＣカードに対して指定キー番号を送信する第１の送信手段と、
上記キーカードへ指定コマンド番号と実行パラメータと指定キー番号とを送信する第２の送信手段と、
この第２の送信手段に応答して上記キーカードから得られる暗号化済みコマンドを上記ＩＣカードへ送信する第３の送信手段とからなり、
上記ＩＣカードが、
指定キー番号に対応する種々の暗号化キーを記憶している第２の記憶手段と、
上記ＩＣカード処理装置からの指定キー番号に対応する

暗号化キーを上記第２の記憶手段により読出し、この読出した暗号化キーに基づいて上記ＩＣカード処理装置からの暗号化されたコマンド電文を復号化する復号化手段と、
この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる、
ことを特徴とするＩＣカード処理システム。
【請求項１１】　ＩＣカードの発行を指示するＩＣカード処理装置と、このＩＣカード処理装置による指示とキーカードからのデータに基づいてＩＣカードを発行するリーダライタとからなるＩＣカード処理システムにおいて、
上記ＩＣカード処理装置が、
ＩＣカードの発行指示を上記リーダライタへ送信する第１の送信手段からなり、
上記リーダライタが、
ＩＣカードへ送信するコマンド電文を生成する生成手段と、
上記ＩＣカード処理装置からのＩＣカードの発行指示に基づいて、上記キーカードより暗号化キーを読出し、この読出した暗号化キーにより上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、
この暗号化手段により暗号化されたコマンド電文と上記暗号化キーを上記ＩＣカードへ送信する第２の送信手段とからなり、
上記キーカードが、
暗号化キーを記憶する記憶手段と、
上記リーダライタからの指示に基づいて暗号化キーを上記リーダライタへ送信する第３の送信手段とからなり、
上記ＩＣカードが、
上記リーダライタからの暗号化キーに基づいて、上記リーダライタからの暗号化されたコマンド電文を復号化する復号化手段と、
この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる、
ことを特徴とするＩＣカード処理システム。
【請求項１２】　ＩＣカードの発行を指示するＩＣカード処理装置と、このＩＣカード処理装置による指示とキーカードからのデータに基づいてＩＣカードを発行するリーダライタとからなるＩＣカード処理システムにおいて、
上記ＩＣカード処理装置が、
ＩＣカードの発行指示を上記リーダライタへ送信する第１の送信手段からなり、
上記リーダライタが、
ＩＣカードへ送信するコマンド電文を生成する生成手段と、
上記ＩＣカード処理装置からのＩＣカードの発行指示に基づいて、上記キーカードより暗号化キーを読出し、この読出した暗号化キーにより上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、
この暗号化手段により暗号化されたコマンド電文を上記ＩＣカードへ送信する第２の送信手段とからなり、
上記キーカードが、
暗号化キーを記憶する記憶手段と、
上記リーダライタからの指示に基づいて暗号化キーを上記リーダライタへ送信する第３の送信手段とからなり、
上記ＩＣカードが、
上記リーダライタからの暗号化されたコマンド電文を復号化する復号化手段と、
この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる、
ことを特徴とするＩＣカード処理システム。
【請求項１３】　ＩＣカード処理装置とＩＣカードとからなるＩＣカード処理方法において、
上記ＩＣカード処理装置が、
ＩＣカードに対してカード固有番号の出力要求を上記ＩＣカードへ送信し、
この送信に応答して得られるＩＣカードのカード固有番号を暗号キーとしてコマンド電文を暗号化し、
この暗号化されたコマンド電文を上記ＩＣカードへ送信し、
上記ＩＣカードが、
カード固有番号を記憶している記憶手段と、
上記ＩＣカード処理装置からのカード固有番号の出力要求に応答してあらかじめ記憶されているカード固有番号を上記ＩＣカード処理装置へ送信し、
この送信に応答して得られる暗号化されたコマンド電文を上記カード固有番号を復号キーとして復号化し、
この復号化されたコマンド電文に基づいた処理を行う、
ことを特徴とするＩＣカード処理方法。
【請求項１４】　カード固有情報を記憶している記憶手段と、
カード発行装置から暗号化されて送信されるファイル創生コマンドを前記記憶手段に記憶しているカード固有情報を復号キーとして復号する復号化手段と、
この復号化手段により復号化されたファイル創生コマンドによりファイルの創生を行なうファイル創生手段と、
このファイル創生手段によるファイル創生が完了した場合上記カード発行装置から暗号化されて送信されるファイル創生コマンドを受付けないようにしたことを特徴とするＩＣカード。
【請求項１５】　請求項１４のＩＣカードにおいて、
上記ファイル創生手段により特定ファイルが生成された場合にファイル生成が完了したことを検出する手段を有し、ファイル生成の完了が検出された場合、以後上記カード発行装置から暗号化されて送信されるファイル創生コマンドを受付けないようにしたことを特徴とするＩＣカード。
【請求項１６】　請求項１４のＩＣカードにおいて、

上記ファイル創生手段により特定ファイルが生成された場合にファイル生成が完了したことを検出する手段を有し、ファイル生成の完了が検出された場合、以後上記カード発行装置から暗号化されて送信されるファイル創生コマンドを受付けないようにしたことを特徴とするＩＣカード。

【請求項１７】　請求項１４のＩＣカードにおいて、上記カード発行装置からの指示に基づき、以後上記カード発行装置から暗号化されて送信されるファイル創生コマンドを受付けないようにしたことを特徴とするＩＣカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ＩＣカードの発行時のコマンド等が隠蔽されるＩＣカード処理装置とＩＣカードとＩＣカード処理システムとＩＣカード処理方法に関する。

【０００２】

【従来の技術】ＩＣカードは、各運用アプリケーションに従って適宜アプリケーションファイルをＩＣのメモリ内に生成し、各種キー情報等をそのファイルに対して設定して使用する。ここでは、このアプリケーションごとに共通のファイル生成・キー設定等を「一次発行」と呼び、この一次発行で生成されたファイルにカード個別のデータを設定する作業を「二次発行」と呼ぶ。

【０００３】さて、この一次発行は、一般的にカードが理解できる「発行コマンド」を使用する。すなわち、アプリケーションから要求される種々の形のファイルの生成や、そのファイルに設定されるキーデータ等をカード（のＯＳ）に対してコマンドの形で示し、カード（のＯＳ）がこれを解釈して内部メモリ上にファイルを生成する。…(1)

また、ＩＣカードに対してＰＣ（パソコン）等の機器がデータを送信する場合、ＰＣ等の機器とカードとの間には、カードを保持してカードに対して電源供給や活性化制御等を行なうリーダライタと呼ばれる機器が介在する必要がある。このリーダライタは多くの場合ＰＣ等とＲＳ－２３２ＣやＳＣＳＩといった通信インタフェースで通信線を介してＰＣ等の機器と接続される。…(2)

さらに、この発行コマンドは、ＰＣ等の機器内のプログラムの一部としてその機器内に格納されており、プログラム動作の一つとしてその機器からカードに向けて送出されることになる。…(3)

ＩＣカード内のファイルが(1)の様に生成されるということは、未発行のカードと発行コマンドに関する情報が手に入れば、いかなるカードも作成出来ることになる。

【０００４】しかしながら、従来よりこの発行コマンドはカードに対してそのパラメータも含めて裸の状態で送られているため、カードへのコマンド電文をカード表面の接点やリーダライタの通信線の伝送データをモニタすること、あるいはＰＣ等の発行コマンドを送出する機器のプログラムを解析することによって、発行コマンド自体だけでなく、各アプリケーションでどの様なファイルが生成され、どの様なキーやパラメータが設定されるのかを解析することができる状態である。

【０００５】現在、発行作業は発行センタといった部外者の立ち入らない、すなわち伝送データのモニタや、機器側プログラムの解析が実行できない環境でのみ行なうことでこの様な問題に対抗して来たが、一アプリケーションで複数の異なるファイル構成のカードを使用したり、カードの発注処理・在庫管理の効率化等の要求から、近年、未発行のカードを出先機関や接客窓口に置き、その場で一次発行から実施する運用の要求があり、この様な場合、前記のカードセンタでの運用の様に(1)～(3)が実行出来ないように管理することは非常に困難になる。

【０００６】

【発明が解決しようとする課題】この発明は、発行対象カードに対する発行コマンド電文を暗号化等の手段により隠蔽することで、未発行のカードを入手して不正にカードを作成しようとする行為に不可欠の発行コマンドに関する情報の漏洩が防止でき、発行処理に関するＩＣカードのセキュリティを向上させることができることを目的とする。

【０００７】さらに、この発明は、コマンド電文の暗号化に関する端末機側の処理に使用するデータ類を発行機システムには一般的なキーカードに格納することで、そのセキュリティをより向上させることができることを目的とする。

【０００８】また、端末機側での暗・復号処理自体をキーカード内で実施することで、そのセキュリティを更に向上させることができることを目的とする。

【０００９】また、この様なキーカードを、キーカードと発行対象のカードの両者を同一筐体内に保持する様な形式のリーダライタで扱う場合、キーカードから出力されるデータをリーダライタ内でクローズして使用することで、そのセキュリティは更に向上することを目的とする。

【００１０】

【課題を解決するための手段】この発明のＩＣカード処理装置は、ＩＣカードへ送信するコマンド電文を生成する生成手段と、ＩＣカードに対してカード固有番号の出力要求を上記ＩＣカードへ送信する第１の送信手段と、この第１の送信手段に応答して得られるＩＣカードのカード固有番号を暗号キーとして上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、この暗号化手段により暗号化されたコマンド電文を上記ＩＣカードへ送信する第２の送信手段と、この第２の送信手段に応答して得られる処理結果に応じて処理を終了する終了手段とからなる。

【００１１】この発明のＩＣカードは、カード固有番号を記憶している記憶手段と、外部装置からのカード固有番号の出力要求に応答して上記記憶手段から読出したカード固有番号を上記外部装置へ送信する第１の送信手段と、この第１の送信手段に応答して得られる暗号化されたコマンド電文を上記記憶手段から読出したカード固有番号を復号キーとして復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段と、この処理手段による処理結果を上記外部装置へ送信する第２の送信手段とからなる。

【００１２】この発明のＩＣカード処理システムは、ＩＣカード処理装置とＩＣカードとからなるものにおいて、上記ＩＣカード処理装置が、ＩＣカードへ送信するコマンド電文を生成する生成手段と、ＩＣカードに対してカード固有番号の出力要求を上記ＩＣカードへ送信する第１の送信手段と、この第１の送信手段に応答して得られるＩＣカードのカード固有番号を暗号キーとして上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、この暗号化手段により暗号化されたコマンド電文を上記ＩＣカードへ送信する第２の送信手段とからなり、上記ＩＣカードが、カード固有番号を記憶している記憶手段と、上記ＩＣカード処理装置からのカード固有番号の出力要求に応答して上記記憶手段から読出したカード固有番号を上記ＩＣカード処理装置へ送信する第３の送信手段と、この第３の送信手段に応答して得られる暗号化されたコマンド電文を上記記憶手段から読出したカード固有番号を復号キーとして復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる。

【００１３】この発明のＩＣカード処理システムは、ＩＣカード処理装置とＩＣカードとからなるものにおいて、上記ＩＣカード処理装置が、ＩＣカードへ送信するコマンド電文を生成する生成手段と、ＩＣカードに対してカード固有番号の出力要求を上記ＩＣカードへ送信する第１の送信手段と、この第１の送信手段に応答して得られるＩＣカードのカード固有番号を暗号キーとして上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、この暗号化手段により暗号化されたコマンド電文を上記ＩＣカードへ送信する第２の送信手段と、この第２の送信手段に応答して得られる処理結果が供給された際に、上記生成手段により生成されたコマンド電文の送信を行うか終了するかを判断する判断手段と、この判断手段によりコマンド電文の送信を判断した際に、上記ＩＣカードのカード固有番号を暗号キーとして上記生成手段により生成されたコマンド電文を上記暗号化手段により暗号化し、上記第２の送信手段により暗号化されたコマンド電文を上記ＩＣカードへ送信する第１の処理手段とからなり、上記ＩＣカードが、カード固有番号を記憶している記憶手段と、上記ＩＣカード処理装置からのカード固有番号の出力要求に応答して上記記憶手段から読出したカード固有番号を上記ＩＣカード処理装置へ送信する第３の送信手段と、この第３の送信手段に応答して得られる暗号化されたコマンド電文を上記記憶手段から読出したカード固有番号を復号キーとして復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う第２の処理手段と、この第２の処理手段による処理結果を上記ＩＣカード処理装置へ送信する第４の送信手段とからなる。

【００１４】この発明のＩＣカード処理システムは、ＩＣカード処理装置とＩＣカードとからなるものにおいて、上記ＩＣカード処理装置が、ＩＣカードへ送信するコマンド電文を生成する第１の生成手段と、ＩＣカードに対して乱数の出力要求を上記ＩＣカードへ送信する第１の送信手段と、この第１の送信手段に応答して得られるＩＣカードからの乱数を暗号キーとして上記第１の生成手段により生成されたコマンド電文を暗号化する暗号化手段と、この暗号化手段により暗号化されたコマンド電文を上記ＩＣカードへ送信する第２の送信手段とからなり、上記ＩＣカードが、カード固有番号を記憶している記憶手段と、この記憶手段から読出したカード固有番号に基づく乱数を生成する第２の生成手段と、上記ＩＣカード処理装置からの乱数の出力要求に応答して上記第２の生成手段により生成される乱数を上記ＩＣカード処理装置へ送信する第３の送信手段と、この第３の送信手段に応答して得られる暗号化されたコマンド電文を上記第２の生成手段により生成される乱数を復号キーとして復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる。

【００１５】この発明のＩＣカード処理システムは、ＩＣカード処理装置とＩＣカードとからなるものにおいて、上記ＩＣカード処理装置が、前回の乱数を記憶する記憶手段と、この記憶手段により読出した前回の乱数に基づく乱数を生成する第１の生成手段と、ＩＣカードへ送信するコマンド電文を生成する第２の生成手段と、上記第１の生成手段により生成される乱数を上記ＩＣカードへ送信する第１の送信手段と、この第１の送信手段に応答して得られるＩＣカードからの処理準備開始応答が供給された際に、上記第１の生成手段により生成される乱数を暗号キーとして上記第２の生成手段により生成されたコマンド電文を暗号化する暗号化手段と、この暗号化手段により暗号化されたコマンド電文を上記ＩＣカードへ送信する第２の送信手段と、この第２の送信手段に応答して得られるＩＣカードからの応答が供給された際に、上記第１の生成手段により生成される乱数を暗号キーとして上記第２の生成手段により生成されたコマンド電文を上記暗号化手段で暗号化し、この暗号化されたコマンド電文を上記ＩＣカードへ上記第２の送信手段で送信する第１の処理手段とからなり、上記ＩＣカードが、上記ＩＣカード処理装置からの乱数に基づいて、処理準

備開始応答を上記ＩＣカード処理装置へ送信する上記第３の送信手段と、上記ＩＣカード処理装置からの乱数に基づいて、上記第３の送信手段に応答して得られる暗号化されたコマンド電文を復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う第２の処理手段と、この第２の処理手段による処理結果を上記ＩＣカード処理装置へ送信する第４の送信手段と、この第４の送信手段に応答して得られる暗号化されたコマンド電文を、上記復号化手段で上記ＩＣカード処理装置からの乱数に基づいて復号化し、この復号化されたコマンド電文に基づいた処理を上記第２の処理手段で行う第３の処理手段とからなる。

【００１６】この発明のＩＣカード処理システムは、ＩＣカード処理装置とＩＣカードとからなるものにおいて、上記キーカードが、上記ＩＣカード処理装置から与えられる前回処理に使用された乱数を記憶する第１の記憶手段、認証データを記憶する第２の記憶手段と、上記ＩＣカード処理装置からの認証データと上記第２の記憶手段に記憶されている認証データとが一致した際に、上記第１の記憶手段に記憶されている前回の乱数を上記ＩＣカード処理装置へ送信する第１の送信手段とからなり、上記ＩＣカード処理装置が、上記キーカードへ認証データを送信する第２の送信手段と、この第２の送信手段に応答して上記キーカードから得られる前回の乱数に基づく乱数を生成する第１の生成手段と、この第１の生成手段で生成された乱数を上記キーカードへ送信する第３の送信手段と、ＩＣカードへ送信するコマンド電文を生成する第２の生成手段と、上記第１の生成手段により生成される乱数を上記ＩＣカードへ送信する第４の送信手段と、この第４の送信手段に応答して得られるＩＣカードからの処理準備開始応答が供給された際に、上記第１の生成手段により生成される乱数を暗号キーとして上記第２の生成手段により生成されたコマンド電文を暗号化する暗号化手段と、この暗号化手段により暗号化されたコマンド電文を上記ＩＣカードへ送信する第５の送信手段と、この第５の送信手段に応答して得られるＩＣカードからの応答が供給された際に、上記第１の生成手段により生成される乱数を暗号キーとして上記第２の生成手段により生成されたコマンド電文を上記暗号化手段で暗号化し、この暗号化されたコマンド電文を上記ＩＣカードへ上記第５の送信手段で送信する第１の処理手段とからなり、上記ＩＣカードが、上記ＩＣカード処理装置からの乱数に基づいて、処理準備開始応答を上記ＩＣカード処理装置へ送信する上記第６の送信手段と、上記ＩＣカード処理装置からの乱数に基づいて、上記第６の送信手段に応答して得られる暗号化されたコマンド電文を復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う第２の処理手段と、この第２の処理手段による処理結果を上記ＩＣカード処理装置へ送信する第７の送信手段と、この第７の送信手段に応答して得られる暗号化されたコマンド電文を、上記復号化手段で上記ＩＣカード処理装置からの乱数に基づいて復号化し、この復号化されたコマンド電文に基づいた処理を上記第２の処理手段で行う第３の処理手段とからなる。

【００１７】この発明のＩＣカード処理システムは、ＩＣカード処理装置とＩＣカードとからなるものにおいて、上記キーカードが、指定コマンド番号が付与されている種々のコマンド形式と実行パラメータに応じたコマンドを記憶する第１の記憶手段と、上記ＩＣカード処理装置からの指定コマンド番号と実行パラメータに対応するコマンドを上記第１の記憶手段から読出し、この読出したコマンドを上記ＩＣカード処理装置からの暗号キーに基づいて暗号化する暗号化手段と、この暗号化手段により暗号化した暗号化済みコマンドを上記ＩＣカード処理装置へ送信する第１の送信手段とからなり、上記ＩＣカード処理装置が、上記ＩＣカードに対してカード固有番号の出力要求を送信する第１の送信手段と、上記キーカードへ指定コマンド番号と実行パラメータと上記第１の送信手段に応答して得られるＩＣカードのカード固有番号としての暗号キーを送信する第２の送信手段と、この第２の送信手段に応答して上記キーカードから得られる暗号化済みコマンドを上記ＩＣカードへ送信する第３の送信手段とからなり、上記ＩＣカードが、カード固有番号を記憶している第２の記憶手段と、上記ＩＣカード処理装置からのカード固有番号の出力要求に応答して上記第２の記憶手段から読出したカード固有番号を上記ＩＣカード処理装置へ送信する第３の送信手段と、この第３の送信手段に応答して得られる暗号化されたコマンド電文を上記第２の記憶手段から読出したカード固有番号を復号キーとして復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる。

【００１８】この発明のＩＣカード処理システムは、ＩＣカード処理装置とＩＣカードとからなるものにおいて、上記キーカードが、指定コマンド番号が付与されている種々のコマンド形式と実行パラメータに応じたコマンドと、指定キー番号に対応する種々の暗号化キーを記憶する第１の記憶手段と、上記ＩＣカード処理装置からの指定コマンド番号と実行パラメータに対応するコマンドを上記第１の記憶手段から読出し、上記ＩＣカード処理装置からの指定キー番号に対応する暗号化キーを読出し、この読出したコマンドを読出した暗号化キーに基づいて暗号化する暗号化手段と、この暗号化手段により暗号化した暗号化済みコマンドを上記ＩＣカード処理装置へ送信する第１の送信手段とからなり、上記ＩＣカード処理装置が、上記キーカードへ指定コマンド番号と実行パラメータと指定キー番号とを送信する第１の送信手段と、この第１の送信手段に応答して上記キーカードから得られる暗号化済みコマンドを上記ＩＣカードへ送信す

る第３の送信手段とからなり、上記ＩＣカードが、暗号化キーを記憶している第２の記憶手段と、上記暗号化キーを上記第２の記憶手段により読出し、この読出した暗号化キーに基づいて上記ＩＣカード処理装置からの暗号化されたコマンド電文を復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる。

【００１９】この発明のＩＣカード処理システムは、ＩＣカード処理装置とＩＣカードとからなるものにおいて、上記キーカードが、指定コマンド番号が付与されている種々のコマンド形式と実行パラメータに応じたコマンドと、指定キー番号に対応する種々の暗号化キーを記憶する第１の記憶手段と、上記ＩＣカード処理装置からの指定コマンド番号と実行パラメータに対応するコマンドを上記第１の記憶手段から読出し、上記ＩＣカード処理装置からの指定キー番号に対応する暗号化キーを読出し、この読出したコマンドを読出した暗号化キーに基づいて暗号化する暗号化手段と、この暗号化手段により暗号化した暗号化済みコマンドを上記ＩＣカード処理装置へ送信する第１の送信手段とからなり、上記ＩＣカード処理装置が、上記ＩＣカードに対して指定キー番号を送信する第１の送信手段と、上記キーカードへ指定コマンド番号と実行パラメータと指定キー番号とを送信する第２の送信手段と、この第２の送信手段に応答して上記キーカードから得られる暗号化済みコマンドを上記ＩＣカードへ送信する第３の送信手段とからなり、上記ＩＣカードが、指定キー番号に対応する種々の暗号化キーを記憶している第２の記憶手段と、上記ＩＣカード処理装置からの指定キー番号に対応する暗号化キーを上記第２の記憶手段により読出し、この読出した暗号化キーに基づいて上記ＩＣカード処理装置からの暗号化されたコマンド電文を復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる。

【００２０】この発明のＩＣカード処理システムは、ＩＣカードの発行を指示するＩＣカード処理装置と、このＩＣカード処理装置による指示とキーカードからのデータに基づいてＩＣカードを発行するリーダライタとからなるものにおいて、上記ＩＣカード処理装置が、ＩＣカードの発行指示を上記リーダライタへ送信する第１の送信手段からなり、上記リーダライタが、ＩＣカードへ送信するコマンド電文を生成する生成手段と、上記ＩＣカード処理装置からのＩＣカードの発行指示に基づいて、上記キーカードより暗号化キーを読出し、この読出した暗号化キーにより上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、この暗号化手段により暗号化されたコマンド電文と上記暗号化キーを上記ＩＣカードへ送信する第２の送信手段とからなり、上記キーカードが、暗号化キーを記憶する記憶手段と、上記リーダライタからの指示に基づいて暗号化キーを上記リーダライタへ送信する第３の送信手段とからなり、上記ＩＣカードが、上記リーダライタからの暗号化キーに基づいて、上記リーダライタからの暗号化されたコマンド電文を復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる。

【００２１】この発明のＩＣカード処理システムは、ＩＣカードの発行を指示するＩＣカード処理装置と、このＩＣカード処理装置による指示とキーカードからのデータに基づいてＩＣカードを発行するリーダライタとからなるものにおいて、上記ＩＣカード処理装置が、ＩＣカードの発行指示を上記リーダライタへ送信する第１の送信手段からなり、上記リーダライタが、ＩＣカードへ送信するコマンド電文を生成する生成手段と、上記ＩＣカード処理装置からのＩＣカードの発行指示に基づいて、上記キーカードより暗号化キーを読出し、この読出した暗号化キーにより上記生成手段により生成されたコマンド電文を暗号化する暗号化手段と、この暗号化手段により暗号化されたコマンド電文を上記ＩＣカードへ送信する第２の送信手段とからなり、上記キーカードが、暗号化キーを記憶する記憶手段と、上記リーダライタからの指示に基づいて暗号化キーを上記リーダライタへ送信する第３の送信手段とからなり、上記ＩＣカードが、上記リーダライタからの暗号化キーに基づいて、上記リーダライタからの暗号化されたコマンド電文を復号化する復号化手段と、この復号化手段により復号化されたコマンド電文に基づいた処理を行う処理手段とからなる。

【００２２】この発明のＩＣカードは、カード固有情報を記憶している記憶手段と、カード発行装置から暗号化されて送信されるファイル創生コマンドを前記記憶手段に記憶しているカード固有情報を復号キーとして復号する復号化手段と、この復号化手段により復号化されたファイル創生コマンドによりファイルの創生を行なうファイル創生手段と、このファイル創生手段によるファイル創生が完了した場合上記カード発行装置から暗号化されて送信されるファイル創生コマンドを受付けないようにしている。

【００２３】

【発明の実施の形態】以下、図面を参照してこの発明のＩＣカード処理システムとしてのＩＣカード発行システムを説明する。

【００２４】このＩＣカード発行システムは、出先機関や接客窓口に設置した不特定多数の人間が触れることができる環境で運用される機器により構成され、伝送データのモニタや、機器側プログラムの解析を回避することがなされている。

【００２５】図１は、この発明のＩＣカード発行システムのブロックを示している。

【００２６】この実施形態では、コマンド電文自体を、受信したカードだけしか解釈する事ができない形式に暗

号化してカードに対して送信することにより、カードへのコマンド電文をモニタしても、発行コマンドに関する情報の漏洩が防止でき、発行処理に関するＩＣカードのセキュリティを向上できる。未発行のカードを入手して不正にカードを作成しようとする行為に不可欠の発行コマンドに関する情報の漏洩が防止できる。

【００２７】このＩＣカード発行システムは、図１に示すように、パソコン（ＰＣ）１とこのＰＣ１と通信ライン２を介して接続されているリーダライタ３とからなる。このリーダライタ３には、図示しないコネクタ等で接続される発行対象カードとしてのＩＣカード４が装着されるようになっている。

【００２８】ＰＣ１は、ＰＣ１の全体を制御する制御部５、制御用のプログラムが記憶されていたり種々のデータが記憶されるメモリ６、操作指示を行うキーボード等の操作部７、操作案内等が表示される表示部８、リーダライタ３とのデータのやり取りを行うインターフェース９により構成されている。

【００２９】上記制御部５としては、ＩＣカード４から供給される製造番号（カード固有情報）を暗号キーとしてコマンド電文の暗号化を行う暗号化機能を有している。メモリ６から読取った各カードに対する共通の暗号キーとしてコマンド電文の暗号化を行う暗号化機能（第１の実施形態）、ＩＣカード４から供給される製造番号を暗号キーとしてコマンド電文の暗号化を行う暗号化機能（第２の実施形態）、ＩＣカード４から供給される乱数を暗号キーの種としてコマンド電文の暗号化を行う暗号化機能（第３の実施形態）を有し、上記暗号化プログラム（制御部処理プログラム）はＲＯＭ１５に格納されている。また、上記ＣＰＵ１４は、生成された乱数を格納する乱数バッファをメモリ６に用意している（第３、第４の実施形態）。

【００３０】リーダライタ３は、リーダライタ３の全体を制御するＣＰＵ１０、制御用のプログラムが記憶されていたり種々のデータが記憶されるメモリ１１、ＰＣ１とのデータのやり取りを行うインターフェース１２、ＩＣカード４とのデータのやり取りを行うインターフェース１３により構成されている。また、リーダライタ３には、ＩＣカード４の挿入検知を行う検知器（図示しない）を有し、この検知結果をＰＣ１へ出力するようになっている。また、リーダライタ３は、ＩＣカード４の挿入検知時にＩＣカード４の内容を読取り、アプリケーション等が未記録の発行用のカードか否かを示すデータをＰＣ１へ出力するようにしても良い。

【００３１】ＩＣカード４は、図２に示すように、ＩＣカード４の全体を制御するＣＰＵ１４、カード内部動作の制御用のプログラムが記憶されているＲＯＭ１５、外部（リーダライタ３）と交換する電文の送受信バッファとＣＰＵ１４の処理中のデータの一時格納バッファとして利用されるＲＡＭ１６、アプリケーション運用でその値内容をリードライトして使用される運用データが格納され、電文隠蔽用キーデータとしてのカード固有の製造番号等が格納されるＥＥＰＲＯＭ１７、リーダライタ３とのデータのやり取りを行うインターフェース１８により構成されている。

【００３２】上記ＣＰＵ１４としては、ＥＥＰＲＯＭ１７から読取った各カードで共通の復号キーとして暗号化済みのコマンド電文の復号化を行う復号化機能（第１の実施形態）、ＥＥＰＲＯＭ１７から読取った製造番号を復号キーとして暗号化済みのコマンド電文の復号化を行う復号化機能（第２の実施形態）、ＥＥＰＲＯＭ１７から読取った製造番号に基づいて乱数生成ロジックにより生成される乱数を復号キーの種として暗号化済みのコマンド電文の復号化を行う復号化機能（第３の実施形態）を有し、上記復号化プログラム（ＣＰＵ処理プログラム）はＲＯＭ１５に格納されている。また、上記ＥＥＰＲＯＭ１７には、乱数を格納する乱数バッファが設けられている（第３、第４の実施形態）。

【００３３】ＰＣ１は、図３に示すように、主制御プログラム、発行コマンドテンプレート、発行情報ファイル等の機能を有している。発行コマンドテンプレートは、図４に示すような、各コマンド種別ごとにカードが解釈できるコマンド電文フォーマットの平文形式でのテンプレートである。主制御プログラムは、外部から記憶媒体や通信等でＰＣ１に一対して与えられる発行情報ファイルの内容に従ってコマンドテンプレートから適用されるものを選択し、発行情報ファイル内のパラメータをテンプレートにセットして平文のコマンド電文を完成させた上でそれを暗号化してから発行対象カード（ＩＣカード４）が装着されているリーダライタ３を経由して発行対象カード（ＩＣカード４）に対して送信するようになっている。

【００３４】図４に示す、コマンドテンプレートとしては、フォルダ／ファイル生成コマンドテンプレートとキー設定コマンドテンプレートとからなる。フォルダ／ファイル生成コマンドテンプレートは、フォルダ／ファイル生成コマンドコード、フォルダ／ファイル指定（実行パラメータ）、フォルダ／ファイル管理情報（処理用データ）により構成され、キー設定コマンドテンプレートは、キー設定コマンドコード、キーファイル（ＩＤ）指定（実行パラメータ）、キーデータ長（処理用データ）、実キーデータ部（処理用データ）により構成されている。

【００３５】図５は、ＩＣカード４に対するコマンド電文の一般形の例を示す。このコマンド電文は、先頭符号２１、送信電文長２２、コマンドコード２３、実行パラメータ２４、処理用データ２５、末尾符号２６により構成されている。先頭符号２１、送信電文長２２、末尾符号２６は、実際のコマンドを示すブロック（コマンドコード２３、実行パラメータ２４、処理用データ２５；コ

マンド処理内容表示部分）を運ぶために標準規格化されているプロトコルで規定される部分（トレーラ）であり、暗号化の対象とはならない。

【００３６】なお、一般的にはそのコマンド電文が暗号化されたものか否かを示す必要があり、その様な情報は先頭符号２１を２種規定し平文と暗号文とで使い分ける方法が用いられる。または、受信されたコマンド電文をとりあえず平文としてとらえて、解釈不能の時にだけ暗号文としての処理を試行するという方法を用いても良い。但し、その際には暗号化の際に暗号化後の電文が平文のコマンド電文と全く同一とならないようにする。

【００３７】上記トレーラで運ばれるブロックの内容のうち、コマンドコード２３はＩＣカード４に対して要求する処理の種別（発行コマンドの例では「ファイルの創成」等）を表し、実行パラメータ２４はコマンドコードで示された処理種別の中での処理内容の詳細パラメータ（発行コマンドの「ファイル創成」の例では「創成するファイルの種類」等）を表し、処理用データ２５はコマンドコードで示された処理種別の中での処理パラメータだけでは表しきれない付帯情報（発行コマンドの「ファイル創成」の例では「創成するファイルの名前やサイズ」等）を表す。これらが暗号化対象となり、暗号化済みのコマンド電文は図６に示すように、先頭符号２１、送信電文長２２、コマンドコード２３と実行パラメータ２４と処理用データ２５とのブロックを暗号化したデータ２７、末尾符号２６により構成される。

【００３８】このとき、暗号化前後で送信電文長２２すなわちコマンド処理を示すブロックの暗号化前後の長さは、同じあるいは変化するようになっている。

【００３９】上記ＩＣカード１のＥＥＰＲＯＭ１７内に格納するデータは、図７に示す様なＰＣ１と類似のフォルダ、ファイルのツリー構造イメージで管理される。

【００４０】図７は、３アプリケーションすなわち３種のサービスが相乗りしたカードを想定している。

【００４１】ここで言うアプリケーションとは、たとえば、買い物金額に応じてポイントが与えられる百貨店の会員システムに、座席予約情報やマイレッジといったデータを格納し利用する旅客航空会社の会員システムと、トレーニング履歴や健康診断情報を蓄積していき健康増進に役立てるフィットネスクラブの会員システムが相乗りしたイメージととらえる。

【００４２】すると、アプリケーションフォルダ１が百貨店用、アプリケーションフォルダ２が航空会社用、アプリケーションフォルダ３がフィットネスクラブ用である。

【００４３】航空会社用のフォルダ２の配下にある各データファイルは航空会社が管理する会員情報と座席予約情報を格納し、アプリケーションフォルダ２’は特にマイレッジ関係のデータを格納するために利用されるものととらえることができる。

【００４４】次に、これらのフォルダ、ファイルの管理情報の例を図８、図９、図１０に示す。

【００４５】まず、図８はアプリケーションフォルダの管理情報の例である。このアプリケーションフォルダ管理情報は、フォルダ名称、フォルダサイズ、上位フォルダ、参照アクセス権、および変更アクセス権により構成されている。

【００４６】フォルダ名称としては、たとえば百貨店の会員システム用フォルダなら百貨店名としたり、何らかの任意の文字列を当てることができる。フォルダを識別するためのものなので１枚のカード内のフォルダの名称は全て異ならなければならないが、全てのカードについて各アプリケーション用のフォルダ名称は同一となっている。

【００４７】フォルダサイズは、配下に生成される全ファイルを格納するのに足るメモリ容量を示す。ＩＣカード４のＥＥＰＲＯＭ１７内へのファイル生成の手順としては、まず各アプリケーション用フォルダを生成して次のステップとして各フォルダ配下にフォルダないしはファイルを生成していくことになる。このため、各アプリケーション用フォルダが必要とするメモリ容量をＥＥＰＲＯＭ１７上に確保するのにこのサイズ情報が必要となる。

【００４８】上位フォルダは、たとえば図７のアプリケーション２フォルダ配下にアプリケーション２’フォルダを生成する様な場合、アプリケーション２’フォルダ生成タイミングでアプリケーション２フォルダを上位フォルダとして指定する。

【００４９】アプリケーション１～３の各フォルダ生成時には、マスタフォルダを上位フォルダとして指定する。

【００５０】参照アクセス権および変更アクセス権は、そのフォルダ内にデータファイルやキーファイルを参照あるいは、生成、削除等するのに先だって照合済みあるいは認証済みの状態にされていなければならないキーがどれであるかを示す。

【００５１】マスタフォルダ配下のアプリケーション用フォルダでは、マスタフォルダ直下のマスタファイル用キーフォルダのいずれかを、また、アプリケーション２’フォルダにおいてはアプリケーション２フォルダ直下のアプリケーション２用キーフォルダのいずれかを指定することになる。

【００５２】たとえば、マスタフォルダ直下のギーデータファイルに対する各アクセス権は、ＥＥＰＲＯＭ１７の特定アドレスにデータを直接書き込む様な方法により製造段階に与えるキーにより管理される。

【００５３】次に、図９はキーファイルの管理情報の例である。キーファイル管理情報は、ファイルＩＤ、キーデータ長、キー種別、参照アクセス権、および変更アクセス権により構成されている。

【００５４】あるキーを特定してアクセスするため各キーにはファイル１Ｄが付与される。但し、異なるアプリケーションフォルダ内のキーについては、アプリケーションフォルダを指定することで区別ができるため同一のキーＩＤを付与することも許容される。

【００５５】また、ＩＣカード４ではキーデータは可変長であり、キーデータ長でそのキーデータの長さを示す。

【００５６】キー種別とは、単純に外部から与えられたキー値と比較される照合用のキーデータなのか、外部から与えられた数値と比較するために先に出力している乱数をカード内部で暗号化する際に使用するためのキーデータとして使用する認証用のキーデータなのかを示す。

【００５７】参照アクセス権は、そのキーの照合処理あるいは認証処理を実行するために必須の他のキーの照合済みあるいは認証済み状態を示す。

【００５８】変更アクセス権は、先に設定されているキーデータ自体を変更する際に必須の他のキーの照合済みあるいは認証済み状態を示す。

【００５９】次に、図１０はデータファイルの管理情報の例である。データファイル管理情報は、ファイルＩＤ、ファイルサイズ、ファイル種別、参照アクセス権、および変更アクセス権により構成されている。

【００６０】ファイルＩＤについてはキーデータファイルと同一の考え方で付与される。またアプリケーション運用に使用されるデータは用途ごとにデータの長さがあらかじめ想定されているため、それに合わせてファイルサイズを示す。

【００６１】ファイル種別とは、ファイルデータの管理方法として、単純なデータの羅列としてメモリ空間を解放するだけのファイルなのか、データをレコードイメージで区切ってカード内でアクセス管理するファイルなのかを示す。

【００６２】参照アクセス権は、そのデータの参照すなわち読み出しを実行するために必須の他のキーの照合済みあるいは認証済み状態を示す。

【００６３】変更アクセス権は、変更すなわち書き換えを実行する際に必須の他のキーの照合済みあるいは認証済み状態を示す。

【００６４】上記各管理情報をＩＣカード４に対してコマンド電文で送り込むことがＩＣカード４の一次発行処理となる。

【００６５】すなわち、図４の様に図５のコマンド電文の処理用データとして上記管理情報を与え、コマンドコードと実行パラメータを図４の様に設定してＩＣカード４に対して送信することで、ＩＣカード４は管理情報に従ってＥＥＰＲＯＭ１７内にメモリ空間を確保し各ファイルを設定していく。

【００６６】次に、通信ライン２におけるコマンド電文を暗号化する方法について説明する。

【００６７】まず、第１の実施形態として、最も簡単な方法について説明する。

【００６８】すなわち、図１に示す構成において、カード製造時に全てのＩＣカード４に同一の復号ロジックと復号鍵を持たせ、ＩＣカード４に対するコマンド電文を送信するＰＣ１側にも、これらに対応した暗号ロジックと暗号キーを持たせる。

【００６９】すなわち、一次発行処理では全てのＩＣカード４に対してシステムごとに共通のファイルを創成するため、全てのＩＣカード４に同一の復号ロジック（具体的にはプログラム）と鍵（復号キー）を使用する。この場合、暗号化後のコマンド電文は全てのＩＣカード４に対して同一とはなるが、少なくとも図５の様な裸の状態の「コマンド」を隠蔽することはできる。

【００７０】次に、第２の実施形態として、暗号化したコマンド電文をＩＣカード４ごとに個別にする場合について、図１１に示すフローチャートと図１２に示す状態遷移図を用いて説明する。

【００７１】この場合、ＩＣカード４の個別データとして、製造時にＩＣカード４のＥＥＰＲＯＭ１７に格納される製造番号を利用する。

【００７２】すなわち、一次発行開始時に、ＰＣ１は、ＩＣカード４のＥＥＰＲＯＭ１７から製造番号を読み出し、この値をそのまま、あるいは加工を施した上で暗号化のキーに使用して暗号化したコマンド電文をＩＣカード４に送る。これにより、ＩＣカード４の内部では同様に製造番号を使用して受信したコマンド電文を解釈する。

【００７３】まず、ＰＣ１の表示部８の画面上の発行機アイコンをクリックする（ＳＴ１）。すると、制御部５はＩＣカードの発行を判断し、表示部８により発行用のＩＣカード４のリーダライタ３への挿入要求が表示される（ＳＴ２）。

【００７４】この表示に基づいて、発行用のＩＣカード４がリーダライタ３に挿入される（ＳＴ３）。

【００７５】この挿入の検知信号（リーダライタ３からＰＣ１の制御部５へ出力）に基づいて、制御部５は表示部８により発行機プログラムメインメニューを表示し（ＳＴ４）、発行機アプリケーションを起動する（ＳＴ５）。このメニュー表示により、操作部７により発行カード種別を選択し（ＳＴ６）、一次発行処理を選択する（ＳＴ７）。これにより、制御部５は発行情報ファイルの１ステップ分を取得し、発行コマンドテンプレート選択し、セットし、テンプレートパラメータをセットし、１ステップ分のコマンド電文を生成し、メモリ６に記憶する（ＳＴ８）。

【００７６】この状態において、ＰＣ１の制御部５からＩＣカード４のＣＰＵ１４へ製造番号送出要求が出力される（ＳＴ９）。ＩＣカード４のＣＰＵ１４はＥＥＰＲＯＭ１７に記憶されている製造番号を読出し、ＰＣ１の

制御部５に出力される（ＳＴ１０）。これにより、ＰＣ１の制御部５は供給される製造番号をキーとしてメモリ６に記憶するとともに、その製造番号をキーとして上記メモリ６に記憶されている１ステップ分の発行情報ファイルとしてのコマンド電文を暗号化して暗号化済みコマンド電文を生成し、ＩＣカード４のＣＰＵ１４へ出力される（ＳＴ１１）。ＩＣカード４のＣＰＵ１４はＥＥＰＲＯＭ１７に記憶されている製造番号をキーとして読出し、この読出した製造番号を復号キーとしてＰＣ１からの暗号化済みコマンド電文を復号化することにより（ＳＴ１２）、暗号化されているコマンド電文を解凍し、このコマンドの処理を実行する（ＳＴ１３）。このコマンドによる処理の結果をＰＣ１の制御部５に出力される（ＳＴ１４）。

【００７７】これにより、ＰＣ１の制御部５は処理結果としてのＩＣカード４からのレスポンス電文を受信し（ＳＴ１５）、そのレスポンス内容を確認する（ＳＴ１６）。このレスポンス内容の確認後、次の発行情報ファイルがある場合（ＳＴ１７）、ＰＣ１の制御部５は発行情報ファイルの次の１ステップ分を取得し、発行コマンドテンプレート選択し、セットし、テンプレートパラメータをセットし、１ステップ分のコマンド電文を生成し、メモリ６に記憶する（ＳＴ１８）。

【００７８】これにより、ＰＣ１の制御部５は上記メモリ６に記憶されている次の１ステップ分の発行情報ファイルとしてのコマンド電文を上記メモリ６に記憶されている製造番号をキーとして暗号化して暗号化済みコマンド電文を生成し、ＩＣカード４のＣＰＵ１４へ出力される（ＳＴ１１）。ＩＣカード４のＣＰＵ１４はＥＥＰＲＯＭ１７に記憶されている製造番号をキーとして読出し、この読出した製造番号をキーとしてＰＣ１からの暗号化済みコマンド電文を復号化することにより（ＳＴ１２）、暗号化されているコマンド電文を解凍し、このコマンドの処理を実行する（ＳＴ１３）。このコマンドによる処理の結果がＰＣ１の制御部５に出力される（ＳＴ１４）。

【００７９】これにより、ＰＣ１の制御部５は処理結果としてのＩＣカード４からのレスポンス電文を受信し（ＳＴ１５）、そのレスポンス内容を確認する（ＳＴ１６）。

【００８０】以後、発行情報ファイルのステップ内容がなくなるまで、ステップ１８、１１から１６が繰り返され、上記ステップ１７で次の発行情報ファイルの無しが判断された際に処理を終了する。

【００８１】この例ではＩＣカード４の個別データの分かりやすい代表例として製造番号を使用しているが、コマンド電文の隠蔽を目的とする場合、必ずしもＩＣカード４の製造番号である必要はなく、ＩＣカード４の個別の完全ユニーク性についても必須の条件ではない。

【００８２】次に、第３の実施形態として、暗号化のキーをコマンド電文生成の都度、異ならせる場合について説明する。

【００８３】基本的に一枚のＩＣカード４に対する一次発行処理は、ＩＣカード４のライフサイクルを通して一回だけのものだが、発行コマンドの機能、形式によっては、ＩＣカード４に対して類似のコマンドを多数回送出するケースが考えられる。

【００８４】たとえば、１ファイルの創成について、１回のコマンド送信が必要な場合、創成するファイルの形式に関する情報だけが異なる同一のコマンドを、創成するファイルの数だけ送出するため暗号化された電文の解析の機会が増えることになる。

【００８５】また、キーとして使われる製造番号は一次発行処理の始めの段階で生の値として読み出されるため、複数のＩＣカード４を使用して多数の解析用データを集めることも可能である。

【００８６】このとき、暗号化のキーに製造番号の様な一律の値を使用することは解析の容易性を増すので、解析をより困難にするため、ＩＣカード４内で暗号化に使用する値を都度異ならせる。この場合、各ＩＣカード４のユニーク性を確保するためＩＣカード４の個別の値として製造番号を利用するが、そのままの値ではなく、それを種にして乱数を乱数生成ロジックを利用して生成する。この生成した乱数を次の種にして新たな乱数を乱数生成ロジックを利用して生成する。

【００８７】このように、直前に生成・出力した乱数を次の乱数の種にすることで、都度異なる値（キーとして利用する乱数）が生成される。始めの種がＩＣカード４の個別の値（製造番号）なので、生成される乱数は各ＩＣカード４ごとにも異なる。上記第３の実施形態の一例を、図１３、図１４に示すフローチャートと図１５に示す状態遷移図を用いて説明する。

【００８８】まず、ＰＣ１の表示部８の画面上の発行機アイコンをクリックする（ＳＴ２１）。すると、制御部５はＩＣカードの発行を判断し、表示部８により発行用のＩＣカード４のリーダライタ３への挿入要求が表示される（ＳＴ２２）。

【００８９】この表示に基づいて、発行用のＩＣカード４がリーダライタ３に挿入される（ＳＴ２３）。

【００９０】この挿入の検知信号（リーダライタ３からＰＣ１の制御部５へ出力）に基づいて、制御部５は表示部８により発行機プログラムメインメニューを表示し（ＳＴ２４）、発行機アプリケーションを起動する（ＳＴ２５）。このメニュー表示により、操作部７により発行カード種別を選択し（ＳＴ２６）、一次発行処理を選択する（ＳＴ２７）。これにより、制御部５は発行情報ファイルの１ステップ分を取得し、発行コマンドテンプレート選択し、セットし、テンプレートパラメータをセットし、１ステップ分のコマンド電文を生成し、メモリ６に記憶する（ＳＴ２８）。

【００９１】この状態において、ＰＣ１の制御部５からＩＣカード４のＣＰＵ１４へ乱数送出要求が出力される（ＳＴ２９）。ＩＣカード４のＣＰＵ１４はＥＥＰＲＯＭ１７に記憶されている製造番号を読出し、この読出した製造番号に基づいて乱数生成ロジックにより乱数を生成し、ＥＥＰＲＯＭ１７の乱数バッファに記憶し、その乱数をＰＣ１の制御部５に出力する（ＳＴ３０）。また、ＩＣカード４のＣＰＵ１４はＥＥＰＲＯＭ１７の乱数バッファの乱数に基づいて乱数生成ロジックにより次回に利用する乱数を生成し、乱数バッファに更新記憶する（ＳＴ３１）。

【００９２】また、ＰＣ１の制御部５は供給される乱数を暗号キーとして上記メモリ６に記憶されている１ステップ分の発行情報ファイルとしてのコマンド電文を暗号化して暗号化済みコマンド電文を生成し、ＩＣカード４のＣＰＵ１４へ出力される（ＳＴ３２）。また、ＰＣ１の制御部５は供給される乱数に基づいて乱数生成ロジックにより次回に利用する乱数を生成し、メモリ６の乱数バッファに記憶する（ＳＴ３３）。

【００９３】ＩＣカード４のＣＰＵ１４はＥＥＰＲＯＭ１７の乱数バッファに記憶されている乱数を復号キーとして読出し、この読出した乱数を復号キーとしてＰＣ１からの暗号化済みコマンド電文を復号化することにより（ＳＴ３４）、暗号化されているコマンド電文を解凍し、このコマンドの処理を実行する（ＳＴ３５）。このコマンドによる処理の結果をＰＣ１の制御部５に出力される（ＳＴ３６）。

【００９４】これにより、ＰＣ１の制御部５は処理結果としてのＩＣカード４からのレスポンス電文を受信し（ＳＴ３７）、そのレスポンス内容を確認する（ＳＴ３８）。このレスポンス内容の確認後、次の発行情報ファイルがある場合（ＳＴ３９）、ＰＣ１の制御部５は発行情報ファイルの次の１ステップ分を取得し、発行コマンドテンプレート選択し、セットし、テンプレートパラメータをセットし、１ステップ分のコマンド電文を生成し、メモリ６に記憶する（ＳＴ４０）。

【００９５】これにより、ＰＣ１の制御部５は上記メモリ６に記憶されている次の１ステップ分の発行情報ファイルとしてのコマンド電文を上記メモリ６の乱数バッファに記憶されている乱数を暗号キーとして暗号化して暗号化済みコマンド電文を生成し、ＩＣカード４のＣＰＵ１４へ出力される（ＳＴ４１）。また、ＰＣ１の制御部５はメモリ６の乱数バッファに記憶されている乱数に基づいて乱数生成ロジックにより次回に利用する乱数を生成し、乱数バッファに更新記憶する（ＳＴ４２）。

【００９６】また、ＩＣカード４のＣＰＵ１４はＥＥＰＲＯＭ１７の乱数バッファに記憶されている乱数を復号キーとして読出し、この読出した乱数を復号キーとしてＰＣ１からの暗号化済みコマンド電文を復号化することにより（ＳＴ４３）、暗号化されているコマンド電文を解凍し、このコマンドの処理を実行する（ＳＴ４４）。このコマンドによる処理の結果がＰＣ１の制御部５に出力される（ＳＴ４５）。また、ＩＣカード４のＣＰＵ１４はＥＥＰＲＯＭ１７の乱数バッファの乱数に基づいて乱数生成ロジックにより次回に利用する乱数を生成し、乱数バッファに更新記憶する（ＳＴ４６）。

【００９７】これにより、ＰＣ１の制御部５は処理結果としてのＩＣカード４からのレスポンス電文を受信し（ＳＴ４７）、そのレスポンス内容を確認し（ＳＴ４８）、ステップ３９に戻る。

【００９８】以後、発行情報ファイルのステップ内容がなくなるまで、ステップ３９から４８が繰り返され、上記ステップ３９で次の発行情報ファイルの無しが判断された際に処理を終了する。

【００９９】次に、第４の実施形態として、解析をより困難にするためＩＣカード４内で暗号化に使用する値を都度異ならせる別の手段としてＩＣカード４の個別の製造番号を利用するのではなく、外部からの都度異なるキーを用いる場合について説明する。

【０１００】すなわち、第３の実施形態で使用しているＩＣカード４の製造番号の代わりに、はじめにＰＣ１側から乱数の種をＩＣカード４に対して与え、以降は製造番号を種とするのと同様に直前に生成した乱数を種にしていく方法である。この場合、ＰＣ１側で始めにＩＣカード４に対して与える乱数をＩＣカード４ごとに異ならせることで、上記第３の実施形態のＩＣカード４の製造番号を利用する方法と同様のＩＣカード４の個別性が確保される。ＰＣ１からＩＣカード４に与える乱数を都度異ならせる方法としては、都度ＰＣ１の乱数生成機能を使用する他、直前の発行処理時にＩＣカード４に対して与えた乱数を格納しておいて、これを種に新たな乱数を生成する手法等が考えられる。

【０１０１】また、ＩＣカード４側の処理としては、ＰＣ１から乱数が与えられない限り一次発行処理が開始できない制御とすることで、不正な発行を阻止する効果がより大きくなる。

【０１０２】上記第４の実施形態の一例を、図１６に示すフローチャートと図１７に示す状態遷移図を用いて説明する。ただし、第２の実施形態の図１２のフローチャートと同一部分については同一のステップ番号を付与し説明を省略する。

【０１０３】ステップ８の状態において、ＰＣ１の制御部５は、あらかじめ前回の乱数（メモリ６に記憶）に基づいて乱数生成ロジックにより生成され乱数バッファに記憶されている初期乱数をＩＣカード４のＣＰＵ１４へ出力する（ＳＴ９’）。この新たな乱数生成時に、前回の乱数が更新される。ＩＣカード４のＣＰＵ１４はＥＥＰＲＯＭ１７の一時的乱数バッファに供給される乱数を記憶し、処理準備開始応答をＰＣ１の制御部５へ出力する（ＳＴ１０’）。これにより、ＰＣ１の制御部５は供

給される処理準備開始応答により乱数バッファに記憶されている乱数をキーとして上記メモリ６に記憶されている１ステップ分の発行情報ファイルとしてのコマンド電文を暗号化して暗号化済みコマンド電文を生成し、ＩＣカード４のＣＰＵ１４へ出力される（ＳＴ１１’）。ＩＣカード４のＣＰＵ１４はＥＥＰＲＯＭ１７の一時的乱数バッファに記憶されている乱数をキーとして読出し、この読出した乱数を復号キーとしてＰＣ１からの暗号化済みコマンド電文を復号化することにより（ＳＴ１２’）、暗号化されているコマンド電文を解凍し、このコマンドの処理を実行する（ＳＴ１３）。このコマンドによる処理の結果をＰＣ１の制御部５に出力される（ＳＴ１４）。

【０１０４】これにより、ＰＣ１の制御部５は処理結果としてのＩＣカード４からのレスポンス電文を受信し（ＳＴ１５）、そのレスポンス内容を確認する（ＳＴ１６）。このレスポンス内容の確認後、次の発行情報ファイルがある場合（ＳＴ１７）、ＰＣ１の制御部５は発行情報ファイルの次の１ステップ分を取得し、発行コマンドテンプレート選択し、セットし、テンプレートパラメータをセットし、１ステップ分のコマンド電文を生成し、メモリ６に記憶する（ＳＴ１８）。

【０１０５】これにより、ＰＣ１の制御部５は上記メモリ６に記憶されている次の１ステップ分の発行情報ファイルとしてのコマンド電文を上記メモリ６の乱数バッファに記憶されている乱数をキーとして暗号化して暗号化済みコマンド電文を生成し、ＩＣカード４のＣＰＵ１４へ出力される（ＳＴ１１’）。ＩＣカード４のＣＰＵ１４はＥＥＰＲＯＭ１７の一時的乱数バッファに記憶されている乱数をキーとして読出し、この読出した乱数をキーとしてＰＣ１からの暗号化済みコマンド電文を復号化することにより（ＳＴ１２’）、暗号化されているコマンド電文を解凍し、このコマンドの処理を実行する（ＳＴ１３）。このコマンドによる処理の結果がＰＣ１の制御部５に出力される（ＳＴ１４）。

【０１０６】これにより、ＰＣ１の制御部５は処理結果としてのＩＣカード４からのレスポンス電文を受信し（ＳＴ１５）、そのレスポンス内容を確認する（ＳＴ１６）。

【０１０７】以後、発行情報ファイルのステップ内容がなくなるまで、ステップ１８、１１’、１２’、１３から１６が繰り返され、上記ステップ１７で次の発行情報ファイルの無しが判断された際に処理を終了する。

【０１０８】このようにして、発行処理が終了した際に、制御部５は最終の乱数を前回生成乱数としてメモリ６に記憶するようにしても良い。

【０１０９】上記第４の実施形態の他例を、図１８に示すフローチャートと図１９に示す状態遷移図を用いて説明する。ただし、第３の実施形態の図１３、図１４のフローチャートと同一部分については同一のステップ番号を付与し説明を省略する。

【０１１０】ステップ２８の状態において、ＰＣ１の制御部５はあらかじめ前回の乱数（メモリ６に記憶）に基づいて乱数生成ロジックにより生成される初期乱数をＩＣカード４のＣＰＵ１４へ出力する（ＳＴ２９’）。この新たな乱数生成時に、前回の乱数が更新される。また、ＰＣ１の制御部５は上記初期乱数に基づいて乱数生成ロジックにより生成される乱数をメモリ６の乱数バッファに記憶する（ＳＴ３０’）。ＩＣカード４のＣＰＵ１４は供給される乱数に基づいて乱数生成ロジックにより生成される乱数をＥＥＰＲＯＭ１７の乱数バッファに記憶し、処理準備開始応答をＰＣ１の制御部５へ出力する（ＳＴ３１’）。これにより、ＰＣ１の制御部５は供給される処理準備開始応答によりメモリ６の乱数バッファに記憶されている乱数を暗号キーとして上記メモリ６に記憶されている１ステップ分の発行情報ファイルとしてのコマンド電文を暗号化して暗号化済みコマンド電文を生成し、ＩＣカード４のＣＰＵ１４へ出力する（ＳＴ３２’）。また、ＰＣ１の制御部５はメモリ６の乱数バッファに記憶されている乱数に基づいて乱数生成ロジックにより次回に利用する乱数を生成し、乱数バッファに更新記憶する（ＳＴ３３’）。

【０１１１】ＩＣカード４のＣＰＵ１４はＥＥＰＲＯＭ１７の乱数バッファに記憶されている乱数を復号キーとして読出し、この読出した乱数を復号キーとしてＰＣ１からの暗号化済みコマンド電文を復号化することにより（ＳＴ３４’）、暗号化されているコマンド電文を解凍し、このコマンドの処理を実行する（ＳＴ３５）。このコマンドによる処理の結果をＰＣ１の制御部５に出力される（ＳＴ３６）。また、ＩＣカード４のＣＰＵ１４はＥＥＰＲＯＭ１７の乱数バッファの乱数に基づいて乱数生成ロジックにより次回に利用する乱数を生成し、乱数バッファに更新記憶する（ＳＴ３６’）。

【０１１２】以後、ステップ３７以降は、第３の実施形態の場合と同様である。

【０１１３】上述したようにしてフォルダ、ファイル生成が一旦完了した後は一次発行に使用するコマンドは不要なだけでなく、不正な発行処理を防止する意味でも使用できないようにした方が良い。

【０１１４】上記第１から第４の実施形態では、発行コマンドを暗号化してＩＣカード４に対して与える形式としているため、発行コマンドを使用できなくするための方法として、暗号化されたコマンドを受け付けなくするようにすれば良い。具体的には、発行処理が完了した時点で、マスタフォルダ直下のあるキーをロックあるいは消去するという方法がある。

【０１１５】すなわち、その対象となるキーは発行処理開始時に照合され、ＩＣカード４内で暗号・復号関連機能が動作する際には必ずこのキーの照合状態をチェックし、照合されていないあるいはそのキー自体存在しない

場合にはプログラム動作をスキップする様にしておくことで、暗号化されたコマンドはいっさい受け付けられなくなる。

【０１１６】また、発行処理完了後、一般の運用コマンドについても暗号化機能を利用したい場合は、発行コマンドのコマンドコードを排除する方法を用いても良い。

【０１１７】すなわち、発行コマンドと運用コマンドのコマンドコードを区別しておき（たとえばＩＣカード４内に発行コマンドのコードをテーブル化しておき）受信された暗号化された電文を解釈した結果が発行コマンドの（発行コマンドテーブル内にある）場合、処理不能の応答を返すだけの動作とする。

【０１１８】さらに、発行処理の最終段階としてある特定名称のファイルを生成することで発行処理の完了を示す方法を用いても良い。

【０１１９】すなわち、アプリケーション運用で必要な全てのファイル生成が完了した後、そのＩＣカード４のＲＯＭ１５内のプログラムが認識しているある特定名称のファイルをマスタフォルダ直下に一般のファイル生成コマンドで生成する。ＩＣカード４のプログラムはこのファイルが存在する限り、前記の様な方法で発行コマンドを受け付けない動作を選択することができる。

【０１２０】以上は、コマンドを隠蔽することで伝送データのモニタによる解析を阻止するための方法として、外部機器として想定したＰＣ１内に乱数生成ロジックやコマンドの暗号ロジックおよびコマンドの暗号キーや次のＩＣカード４の発行に使用する前回生成した乱数などを格納する形となっているが、乱数生成や暗号化のロジックはＰＣ１のプログラムの一部として、またキーや乱数データは一般的ＰＣ１のファイルデータとしてそれぞれ格納するイメージとなる。

【０１２１】これらの情報のうち、乱数生成や暗号ロジックはＤＥＳ（デス）といったその論理が公開されているものを使用する場合が多く、プログラム自体を隠蔽することにはあまり意味がなく、そこで使用されるキーデータ、すなわちここでは実際の暗号キーと前回生成乱数こそがセキュリティの要となる。

【０１２２】したがって、これらを一般的ＰＣのファイルとしてＰＣに格納しておくことは危険であり、更にこのキー情報を暗号化したり、キー情報自体を別の媒体に格納してＰＣ自体には残さないようにした方がより効果的である。

【０１２３】以下に、ＩＣカードの発行システムにおいて、キーカードを利用した方法について説明する。

【０１２４】ＩＣカード発行システムにおいて、キーカードは一般的に使用者を制限するために使用される。つまり、発行機を使用する際には、起動時に発行システムのリーダライタに必ず装着しなくてはならないようになっている。このようなキーカードにキーデータを格納・保管し、暗号化等に使用する場合について説明する。

【０１２５】図２０に、暗号化用キーデータも含んだキーカードＣの記憶内容のイメージを示す。

【０１２６】すなわち、キーカードＣの内部構成は、図２に示すＩＣカード４の構成と同様に、ＣＰＵ、ＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭ、インターフェースにより構成されている。

【０１２７】また、キーカードＣには、図２０に示すように、発行者キーと、所持者キーと、発行機プログラム起動用のデータとしてのキーカード身分証明データ、カード所持者氏名・番号データと、コマンド電文隠蔽用のデータとしてのコマンド隠蔽用キーデータ（前回生成乱数）とが記憶されるようになっている。

【０１２８】上記発行者キーと所持者キーの両方がともに照合が一致となった際に、すべてのデータが読出せるようになっている。

【０１２９】上記キーカードＣを用いるＩＣカード発行システムの構成は、図２１に示すように、パソコン（ＰＣ）１とこのＰＣ１と通信ライン２を介して接続されている上記ＩＣカード４の発行用のリーダライタ３と、ＰＣ１と通信ライン３０を介して接続されているキーカードＣ用のリーダライタ３１とからなる。上記リーダライタ３１には、キーカードＣの挿入検知用の検知器（図示しない）が設けられている。なお、図１のＩＣカード発行システムと同一部分については同一符号を付し説明を省略する。

【０１３０】また、キーカードＣ用のリーダライタ３１が通信ライン３０によりＰＣ１と接続される場合について説明したが、図２２に示すように、ＰＣ１のＰＣカードスロット３２に直接、キーカードＣ用のリーダライタ３１が接続（装着）されるようにしても良い。

【０１３１】上記のような構成において、上記キーカードＣを用いたＩＣカードＣの発行について、図２３に示すフローチャートを参照しつつ説明する。

【０１３２】まず、ＰＣ１の表示部８の画面上の発行機アイコンをクリックする（ＳＴ５１）。すると、制御部５はＩＣカードの発行を判断し、表示部８によりキーカードＣのリーダライタ３１への挿入要求が表示される（ＳＴ５２）。

【０１３３】この表示に基づいて、キーカードＣがリーダライタ３１に挿入される（ＳＴ５３）。

【０１３４】この挿入の検知信号（リーダライタ３１からＰＣ１の制御部５へ出力）に基づいて、制御部５はキーカードＣに対して発行機キーとその照合指示とを出力する（ＳＴ５４）。これにより、キーカードＣの制御部は記憶されている発行機キーと供給された発行機キーとが一致するか否かを判断し、一致していた場合、照合ＯＫをＰＣ１へ出力し、不一致の場合、照合ＮＧをＰＣ１へ出力する。

【０１３５】上記ステップ５４の照合指示に基づき、照合ＮＧが返送された場合、制御部５は起動処理を中断す

る。また、上記ステップ５４の照合指示に基づき、照合ＯＫが返送された場合、制御部５は表示部８により所持者キーの入力要求が表示される（ＳＴ５５）。

【０１３６】この表示に基づいて、操作部７により所持者キー（使用者がカード所持者本人で発行機使用有資格者あることを示すための暗証番号）が入力される（ＳＴ５６）。この入力に基づいて、制御部５はキーカードＣに対して所持者キーとその照合指示とを出力する（ＳＴ５７）。これにより、キーカードＣの制御部は記憶されている所持者キーと供給された所持者キーとが一致するか否かを判断し、一致していた場合、照合ＯＫとカード所持者氏名・番号をＰＣ１へ出力し、不一致の場合、照合ＮＧをＰＣ１へ出力する。

【０１３７】上記ステップ５７の照合指示に基づき、照合ＮＧが返送された場合、制御部５は起動処理を中断する。また、上記ステップ５７の照合指示に基づき、照合ＯＫとカード所持者氏名・番号が返送された場合、制御部５は発行機使用履歴リスト（ＥＥＰＲＯＭ内）に自動記録する（ＳＴ５８）。また、制御部５はキーカードＣに対してキーカード身分証明データ（真偽判定のデータ）の読出しを出力する（ＳＴ５９）。これにより、キーカードＣの制御部は記憶されているキーカード身分証明データを読出しＰＣ１へ出力する。

【０１３８】これにより、制御部５は供給されるキーカード身分証明データの内容によりキーカードの真偽を判定する（ＳＴ６０）。

【０１３９】このキーカード身分証明データは、たとえば、そのシステム名称の文字列、システム名称やカード所持者の氏名をビット変換等により暗号化した文字列、あるいはシステム別に割り付けられたそれ自体には意味を持たない乱数値等、外部には明かされないデータである。

【０１４０】ＰＣ１内の発行機プログラム自体が確認するためのものである。

【０１４１】また、実際の発行機プログラム起動処理のコードの一部を格納しておき、カードから読み出してＰＣ１のプログラムの該当部にそれを貼り付ける様な仕組みとすれば、正規の値（コード）がキーカードＣから取り出されなければ、発行機プログラム自体起動できないようにすることができる。プログラムの一部（コード内容）を取出して空白とする。

【０１４２】たとえば、図２４の（ａ）は、制御部５のプログラム処理動作を分かれ道ごとに進行方向を示すことで迷路を抜けるあるいは道路案内をするプログラムにみたてている。実際には分かれ道にさしかかるたびに左側の１から１５に示す方向へ順次進んでいくことで出口あるいは目的地へ到達する事ができるが、途中の７から１０のステップを、図２４の（ｂ）（ｃ）に示すように、キーカードＣに移動してしまい、ＰＣ１のプログラムファイルに残さない様にすることで、決して出口あるいは目的地へは到達できない様になる。

【０１４３】上記ステップ６０の判定結果がＮＧの場合、制御部５は起動処理を中断する。また、上記ステップ６０の判定結果がＯＫの場合、制御部５はキーカードＣに対してコマンド電文隠蔽用のデータとしてのコマンド隠蔽用キーデータ（前回生成乱数）の読出しを出力する（ＳＴ６１）。これにより、キーカードＣの制御部は記憶されているコマンド隠蔽用キーデータを読出しＰＣ１へ出力する。このコマンド隠蔽用キーデータとしての前回生成乱数がＰＣ１に供給され、メモリ６の乱数バッファに記憶されることにより、制御部５は、ＩＣカード４の発行準備が整う（ＳＴ６１）。

【０１４４】この準備が整った後、上記前回生成乱数を用いて上述した第４の実施形態を実施することができる。

【０１４５】すなわち、第４の実施形態では、前回生成乱数がメモリ６に記憶されていたが、上記例ではキーカードＣに記憶されており、発行機の確認（発行機キーの照合）、使用者の暗証照合がなされた後に、キーカードＣから上記前回生成乱数が読出せるようになっているので、前回生成乱数に対するセキュリティが高いものとなっている。

【０１４６】また、ＩＣカード４の発行ごとに制御部５により発行処理により得られた最終の乱数がキーカードＣ内に前回生成乱数として記憶されるようになっている。

【０１４７】また、上記キーカードＣからの真偽判定データの読み出しに続いて、発行コマンドの隠蔽に利用する暗号キーをＰＣ１がキーカードＣから読み出す。すると、ＰＣ１の発行機プログラムはキーカードＣから取り出したキーデータを使用して以降の暗号化、乱数生成の処理を行ない、処理終了と共にキーデータをプログラム上から削除する。処理終了までにキーカードＣ内の格納キーデータを更新する必要があるため、処理の終了時には再度キーカードＣをリーダライタ３１に装着しないと発行機プログラムを終了出来ない様にする。

【０１４８】但し、図２１あるいは図２２の様なキーカード専用のリーダライタ３１が装着された構成の場合、適宜必要なタイミングでキーカードＣにデータを移し、ＰＣ１内にデータを留めない様にすることで、セキュリティをより向上させることができる。

【０１４９】上記したキーカードＣを用いたコマンド電文を隠蔽する方法は、ＰＣ１内に容易にアクセスできる形でセキュリティの要となるデータ（前回生成乱数）を残すことを回避するために、その前回生成乱数をキーカードＣに格納するものである。

【０１５０】しかし、既存のＩＣカードの中には外部から与えられた電文を暗号化する機能を持ったものがある。この機能を利用して、第１から第４の実施形態で用いられている暗号化処理をキーカードＣ内で実施するよ

うにしても良い。

【０１５１】これにより、発行機プログラムの一部としてＰＣ１内にある暗号プログラム自体を隠蔽することが出来るため、ＤＥＳ等の公開されている暗号ロジックだけでなく独自方式の暗号を使用できる。また、キーカードＣにデータを投げ込むだけで暗号化結果が得られるため、暗号発行機プログラムの負荷も軽減される。

【０１５２】具体的には、図１２、図１５、図１７、図１９に示すＰＣ１側における暗号化処理が、キーカードＣ内で行えるようにしている。

【０１５３】このキーカードＣによるデータの暗号化処理を図２５を用いて説明する。

【０１５４】この場合、キーカードＣ内には、指定コマンド番号に対するコマンド形式コマンド種が記憶され、この記憶されているコマンド形式（コマンド種）の１つが選択されている状態において、このコマンド種をＰＣ１から供給される暗号化キーにより暗号化する暗号化プログラムを有している。

【０１５５】すなわち、発行コマンド電文である「暗号化するデータ列」のうち、コマンド形式の主たる部分をキーカードＣ内に格納しておき、ＰＣ１からはその機能番号（指定コマンド番号）と必要なパラメータ（実行パラータ類）だけを渡すことで、キーカードＣ内でＰＣ１で所望の発行コマンドを組み立てた上でさらにそれを暗号化してＰＣ１へ出力することで、発行コマンドは完全に隠蔽される。この暗号化された発行コマンドは発行されるＩＣカード４内で復号化・解釈されて実行されることについては、これまで示した例と変わりはない。

【０１５６】また、図２５では、指定コマンド番号とパラメータ類を別々の矢印で示しているが、実際にカードに対して与える際には一コマンド化するようにしても良い。

【０１５７】このＰＣ１側でのデータの暗号化（キーカードＣによる）は、その時、発行対象となっているＩＣカード４に対して送信されるコマンド電文を隠蔽するためのものなので、発行されるＩＣカード４内で解釈できなければならないようになっている。このため、キーカードＣ側の暗号ロジックと発行されるＩＣカード４側の復号ロジックは対応したものでなければならず、対象となるＩＣカード４を発行するためには対応するキーカードＣが必須となり、セキュリティをより高めることができる。

【０１５８】また、ＰＣ１側プログラムにコマンド電文は持たせないようにでき、ＰＣ１とキーカードＣとの間に通信線があったとしても、コマンド電文は隠蔽されるようになっている。

【０１５９】また、図１５、図１７、図１９に示すＰＣ１側におけるキーを必要としない形の「乱数生成」処理があるが、これも論理的にはある固定の値のキーを使用している暗号化処理の一種と考えることができるため、この乱数生成についてもキーカードＣに委ねるようにしても良い。

【０１６０】このキーカードＣによる乱数生成の処理を、図２６を用いて説明する。

【０１６１】この場合、キーカードＣ内には、図２５の構成にさらに指定キー番号に対応する複数の暗号化キーが記憶され、ＰＣ１からの指定キー番号に対応する暗号化キーが選択され、この選択された暗号化キーにより暗号化プログラムが暗号化を行うようになっている。

【０１６２】すなわち、キーカードＣ内には予め暗号化（乱数生成）のための暗号化キーが格納されており、この暗号化キーを使用して、発行コマンド電文である「暗号化するデータ列」のうち、コマンド形式の主たる部分をキーカードＣ内に格納しておき、ＰＣ１からはその機能番号（指定コマンド番号）と必要なパラメータ（実行パラータ類）だけを渡すことで、キーカードＣ内でＰＣ１で所望の発行コマンドを組み立てた上で、暗号（乱数）化してＰＣ１へ出力する。

【０１６３】カード内の暗号化キーは複数格納することができ、暗号化処理の際にどの暗号化キーを使用するかの指定も可能である。このキーの選択機能を利用して同一キーカードで複数システムに対応することが可能となる。キーカード内にシステム別に複数の暗号化キーを格納した場合、システム別の発行対象カードに適合したキーを指定する必要が発生し、セキュリティをより高めることができる。

【０１６４】この場合、隠蔽すべきデータは全てキーカードＣ内に格納され、発行機プログラムはキーカードＣに対して発行されるカードに対して施したい処理とそれに必要な情報を示すだけで、発行処理が実現される。

【０１６５】なお、図２６では、所望の指定コマンド番号とパラメータ類および指定キー番号を別々の矢印で示しているが、実際にキーカードＣに対して与える際には一コマンド化するようにしても良い。

【０１６６】上述した図２５、図２６の例では、キーカードＣと発行されるＩＣカード４（＝適用システム）が対応づけられる旨の説明を加えたが、これをより強固にしてキーカードＣによるセキュリティ確保の効果を高める方法について説明する。

【０１６７】図１２、図１５では、ＰＣ１側はコマンド電文暗号化用のキーをＩＣカード４から取得し、図１７、図１９ではＰＣ１側で乱数を生成しその値をそのまま、あるいはそれを種にして生成した新たな値を使用して暗号化を実施している。このキーや乱数の初期値を、予めキーカードＣに格納された発行対象のＩＣカード４に関連する情報をもとに生成させることで、事前のデータ交換を不要とする。これによって暗号化されたコマンド送信に先だってコマンド電文の暗号化に使用するデータを交換する方法に比べて、コマンド電文の秘匿に関するセキュリティは更に高くなる。

【０１６８】この方法の簡単な例を、図２７を用いて説明する。

【０１６９】図２５、図２６の例では、発行コマンドをＰＣ１（外部）から与えられるか番号によって指定されたキーにより暗号化しているが、このＰＣ１からの入力無しに適用システム個別のキーデータをキーカードＣと発行対象のＩＣカード４に持ち合い、このキーを使用して、キーカードＣでは発行コマンドを暗号化、発行対象のＩＣカード４では受信した暗号化済み発行コマンドを復号化する。発行対象のＩＣカード４のキーデータは、第１から第４の実施形態と同じく、製造時に適用システム別に格納する。

【０１７０】これにより、発行対象のＩＣカード４は、一次発行処理において、一切の事前手続き無しに暗号化されたコマンド電文を受信してその内容を解釈してコマンド処理を実行できる。

【０１７１】ここまでのキーカードＣの利用方法例は、図２１、図２２の機器構成を前提としてきたが、図２８に示すように、ＰＣ１と一本の通信線Ｓで接続されキーカードＣと発行対象のＩＣカード４の両者が装着できるようなリーダライタ４１を用いても良い。

【０１７２】また、図２９に示すような、発行対象のＩＣカード４が複数枚スタックされており、順次一枚ずつあるいは複数枚取り出されて発行処理が行なわれる様なリーダライタ５０も、キーカードＣの利用については、図２８と同一ととらえることができる。リーダライタ５０は通信線Ｓを介してＰＣ１と接続されている。

【０１７３】このリーダライタ５０は、未発行カードが複数枚スタックされている未発行カードスタック部５１と、この未発行カードスタック部５１から取出された１枚ずつの未発行カードを搬送し、搬送途中にて発行処理を行うカード搬送発行処理部５２と、カード搬送発行処理部５２により発行処理の行われたカードを収納する発行済みカード収納部５３により構成されている。カード搬送発行処理部５２には操作部５４と動作状態表示部５５とキーカードＣ用の差し込み口５６が設けられている。

【０１７４】上記リーダライタ４１、５０においても、これまでに示したキーカードＣの利用例は全て適応できるが、更にこの構成ならでは利用例について次に説明する。

【０１７５】図２１、図２２の構成では、各ＩＣカード４と交換する電文は全てＰＣ１を経由するが、図２８、図２９の構成では、ＩＣカード４の電文をリーダライタ４１、５０内でクローズさせ外部に見えない形とすることができる。

【０１７６】一つの方法としては、図２１の構成と同等の機能を、リーダライタ５０の制御部がＰＣ１の代役を務めることで実現し、リーダライタ４１の制御部が独自にＩＣカード４にアクセスするようにしても良い。

【０１７７】この実現例を、図３０、図３１、図３２を用いて説明する。

【０１７８】すなわち、リーダライタ５０は、リーダライタ５０の全体を制御する制御部５７、未発行カードスタック部５１から発行済みカード収納部５３へＩＣカード４を搬送するカード搬送部５８、カード搬送部５８の途中に設けられる発行対象のＩＣカード４に対してデータのリードライトを行う発行対象のＩＣカード用のリーダライタ部５９、キーカードＣ用の差し込み口５６に差し込まれたキーカードＣに対してデータのリードライトを行うキーカードＣ用のリーダライタ部６０、操作部５４、動作状態表示部５５により構成されている。

【０１７９】このような構成において、カード発行処理時における、ＰＣ１、リーダライタ５０の制御部５７、キーカードＣ、ＩＣカード４とのやりとりの例を、図３１０用いて説明する。

【０１８０】すなわち、ＰＣ１はリーダライタ５０の制御部５７に対して通信線Ｓを通して動作指示を送り、リーダライタ５０の制御部５７が図１２、図１５、図１７、図１９の第１から第４の実施形態に示すＩＣカード４とのやりとりを、図２５、図２６に示すキーカードＣを利用した方法を含めて実施する形となる。

【０１８１】ここで、図２５、図２６中のコマンド形式の表は、図４に示したようなコマンドテンプレートの一覧である。

【０１８２】なお、リーダライタ５０の制御部５７に対するＰＣ１からの動作指示は、ＩＣカード４に対するコマンドと類似の電文による方法で実現できる。

【０１８３】このＰＣ１からリーダライタ５０に対する動作指示（コマンド）電文の例を図３２に示す。図５に示したＩＣカード４に対するコマンド電文に対してコマンドコードが動作種別指示コードに変わっただけのものである。

【０１８４】このコマンド電文は、リーダライタ５０の表示部５５への表示内容、ＩＣカード４の搬送、リーダライタ５０の動作状態の取得等を含むリーダライタ５０本体動作全体に関する動作を指示するためのものである。その動作指示の一つとしてカード発行処理に関する動作指示があり、この場合動作種別指示コードには、キーカードＣの（図２５、図２６のいずれを適用するかといった）使用方法を含めた意味内容のコード割り付けが行われる。動作種別指示コードにキーカードＣの使用方法まで含んだ場合、実行パラメータの中にカードに対するコマンドの種別を入れ、その発行処理で必要な創成するファイルの名前や大きさといった情報を処理用データとして示すようにしても良い。

【０１８５】この様な動作指示（コマンド）電文を使用して、図３０の様な構成の機器でＰＣ１がリーダライタ５０を制御して、図２０のキーカードＣから暗号化されたコマンド電文を取得して発行対象カードに送るのと同

様の処理を実施した際の動作を図３１に示す。

【０１８６】すなわち、ＰＣ１から動作指示（コマンド）電文を受信した、リーダライタ５０の制御部５７は受け取った指示内容に従ってキーカードＣと発行対象のＩＣカード４をアクセスして発行処理を実施し、その実行結果を動作結果通知電文としてＰＣ１に対して返送する。

【０１８７】たとえば、制御部５７はＰＣ１から受け取ったリーダライタ動作指示コマンドを解釈し、このコマンドによりキーカード向けのコマンド電文を生成し、このコマンド電文を用いてキーカードＣに対する処理（要求コマンド種別とパラメータをキーカードＣへ出力）を行い、この処理によりキーカードＣから得られる暗号化済みコマンド電文を用いて発行対象のＩＣカード４に対する処理（はつこう一美コマンド電文をＩＣカード４に出力）を行い、この処理によりＩＣカード４から得られるコマンド実行結果に基づいてＰＣ１向けのレスポンス電文を生成し、この生成したレスポンス電文をリーダライタ動作結果通知としてＰＣ１へ出力する。

【０１８８】もちろん、図２３に示すような発行システム起動時のキーカード処理も、図３１の様なカード発行処理以前に実施されるようになっている。

【０１８９】なお、以上全ての例はＩＣカード発行機システムに限らず、ＩＣカード４に対するコマンド電文を隠蔽したい場合、全てに適用できる。

【０１９０】特に、キーカードＣを使用する方法については、近年登場してきている個人が保有する通常の取引用カードとは別にセキュリティアクセス管理カードを内蔵するような電子マネーのチャージ端末等の、セキュリティアクセス管理カードを発行機システムでのキーカードＣと同様に利用することで同等の機能が実現できる。

【０１９１】この場合、発行機システムでは製造時に格納していたカードあるいはシステム個別のデータは、取引用のカードが利用者個人の手に渡るまでの間に格納されればよい。

【０１９２】上記したように、発行対象のＩＣカードに対する発行コマンド電文を暗号化等の手段により隠蔽することで、未発行のカードを入手して不正にカードを作成しようとする行為に不可欠の発行コマンドに関する情報の漏洩が防止でき、発行処理に関するＩＣカードのセキュリティを向上させることができる。

【０１９３】また、そのコマンド電文の暗号化に関するＰＣ側の処理に使用するデータ類を発行機システムには一般的なキーカードに格納することで、そのセキュリティをより向上させることができる。

【０１９４】また、ＰＣ側での暗・復号処理自体をキーカード内で実施することで、そのセキュリティを更に向上させることができる。

【０１９５】また、この様なキーカードを、キーカードと発行対象のカードの両者を同一筐体内に保持する様な形式のリーダライタで扱う場合、キーカードから出力されるデータをリーダライタ内でクローズして使用することで、そのセキュリティは更に向上する。

【０１９６】

【発明の効果】以上詳述したように、この発明によれば、発行対象カードに対する発行コマンド電文を暗号化等の手段により隠蔽することで、未発行のカードを入手して不正にカードを作成しようとする行為に不可欠の発行コマンドに関する情報の漏洩が防止でき、発行処理に関するＩＣカードのセキュリティを向上させることができる。

【０１９７】また、この発明によれば、コマンド電文の暗号化に関する端末機側の処理に使用するデータ類を発行機システムには一般的なキーカードに格納することで、そのセキュリティをより向上させることができる。

【０１９８】また、この発明によれば、端末機側での暗・復号処理自体をキーカード内で実施することで、そのセキュリティを更に向上させることができる。

【０１９９】また、この発明によれば、この様なキーカードを、キーカードと発行対象のカードの両者を同一筐体内に保持する様な形式のリーダライタで扱う場合、キーカードから出力されるデータをリーダライタ内でクローズして使用することで、そのセキュリティは更に向上することができる。

【図面の簡単な説明】

【図１】この発明のＩＣカード発行システムの構成を示すブロック図。

【図２】ＩＣカードの内部構成を示すブロック図。

【図３】ＰＣの機能を説明するための図。

【図４】発行コマンドテンプレートの構成を説明するための図。

【図５】ＩＣカード４に対するコマンド電文の一般形の例を示す図。

【図６】暗号化済みのコマンド電文の例を示す図。

【図７】ＩＣカードのＥＥＰＲＯＭ内に格納するデータのフォルダ、ファイルのツリー構造を説明するための図。

【図８】アプリケーションフォルダの管理情報の例を示す図。

【図９】キーファイルの管理情報の例を示す図。

【図１０】データファイルの管理情報の例を示す図。

【図１１】第２の実施形態におけるＩＣカードの発行処理を説明するためのフローチャート。

【図１２】第２の実施形態におけるＩＣカードの発行処理を説明するための図。

【図１３】第３の実施形態におけるＩＣカードの発行処理を説明するためのフローチャート。

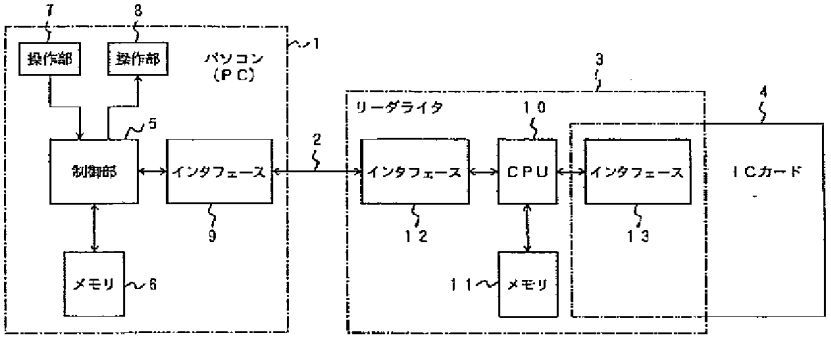
【図１４】第３の実施形態におけるＩＣカードの発行処理を説明するためのフローチャート。

【図１５】第３の実施形態におけるＩＣカードの発行処

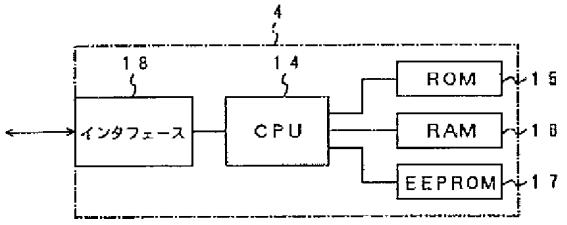
理を説明するための図。
【図１６】第４の実施形態におけるＩＣカードの発行処理を説明するためのフローチャート。
【図１７】第４の実施形態におけるＩＣカードの発行処理を説明するための図。
【図１８】第４の実施形態におけるＩＣカードの発行処理を説明するためのフローチャート。
【図１９】第４の実施形態におけるＩＣカードの発行処理を説明するための図。
【図２０】暗号化用キーデータも含んだキーカードの記憶内容示す図。
【図２１】キーカードを用いるＩＣカード発行システムの構成を示すブロック図。
【図２２】キーカードを用いるＩＣカード発行システムの構成を示す図。
【図２３】キーカードを用いたＩＣカードの発行処理を説明するためのフローチャート。
【図２４】発行機プログラム起動処理のコードの分割記憶を説明するための図。
【図２５】キーカードによるデータの暗号化処理を説明するための図。
【図２６】キーカードによる乱数生成の処理とデータの＊暗号化処理を説明するための図。
【図２７】キーカードとＰＣとＩＣカードのデータのやり取りを説明するための図。
【図２８】ＩＣカード発行システムの構成を示す図。
【図２９】ＩＣカード発行システムの構成を示す図。
【図３０】ＩＣカード発行システムの構成を示すブロック図。
【図３１】ＰＣとリーダライタとキーカードとＩＣカードのデータのやり取りを説明するための図。
【図３２】ＰＣからリーダライタに対するコマンド電文の例を示す図。

【符号の説明】
１…ＰＣ
２…通信ライン
３…リーダライタ
４…ＩＣカード
５…制御部
６…メモリ
１４…ＣＰＵ
１５…ＲＯＭ
１７…ＥＥＰＲＯＭ
Ｃ…キーカード

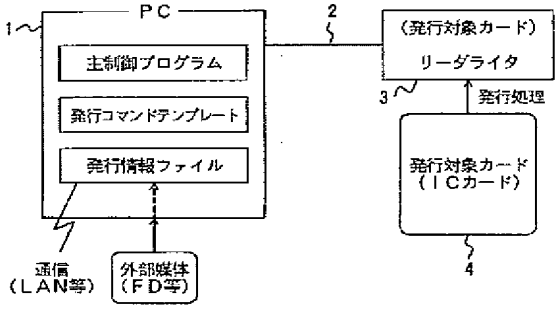
【図１】



【図２】



【図３】



【図４】

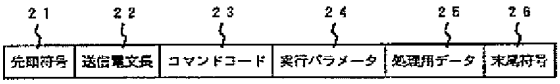
フォルダファイル生成コマンドテンプレート

フォルダ／ファイル生成コマンドコード	フォルダ／ファイル指定	フォルダ／ファイル管理情報

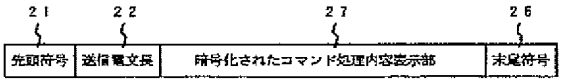
キー設定コマンドテンプレート

キー設定コマンドコード	キーファイル(ＩＤ)指定	キーデータ長　実キーデータ部
コマンド処理内容表示部分		
コマンドコード	実行パラメータ	処理用データ

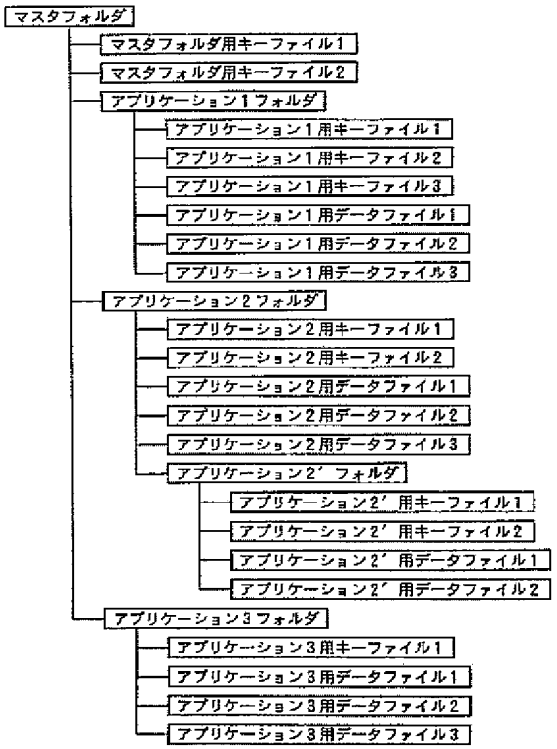
【図５】



【図６】



【図７】



一次発行処理で生成されるファイル構造の一例

【図８】

フォルダ名称	フォルダサイズ	上位フォルダ	参照アクセス権	変更アクセス権

アプリケーションフォルダ管理情報

【図９】

ファイルＩＤ	キーデータ長	キー種別	参照アクセス権	変更アクセス権

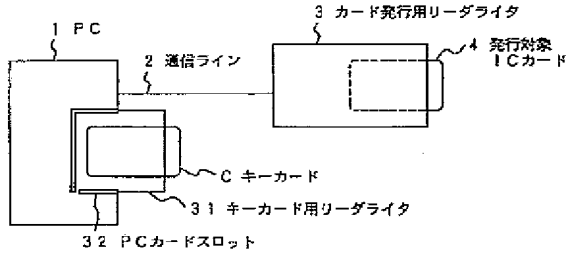
キーデータファイル管理情報

【図１０】

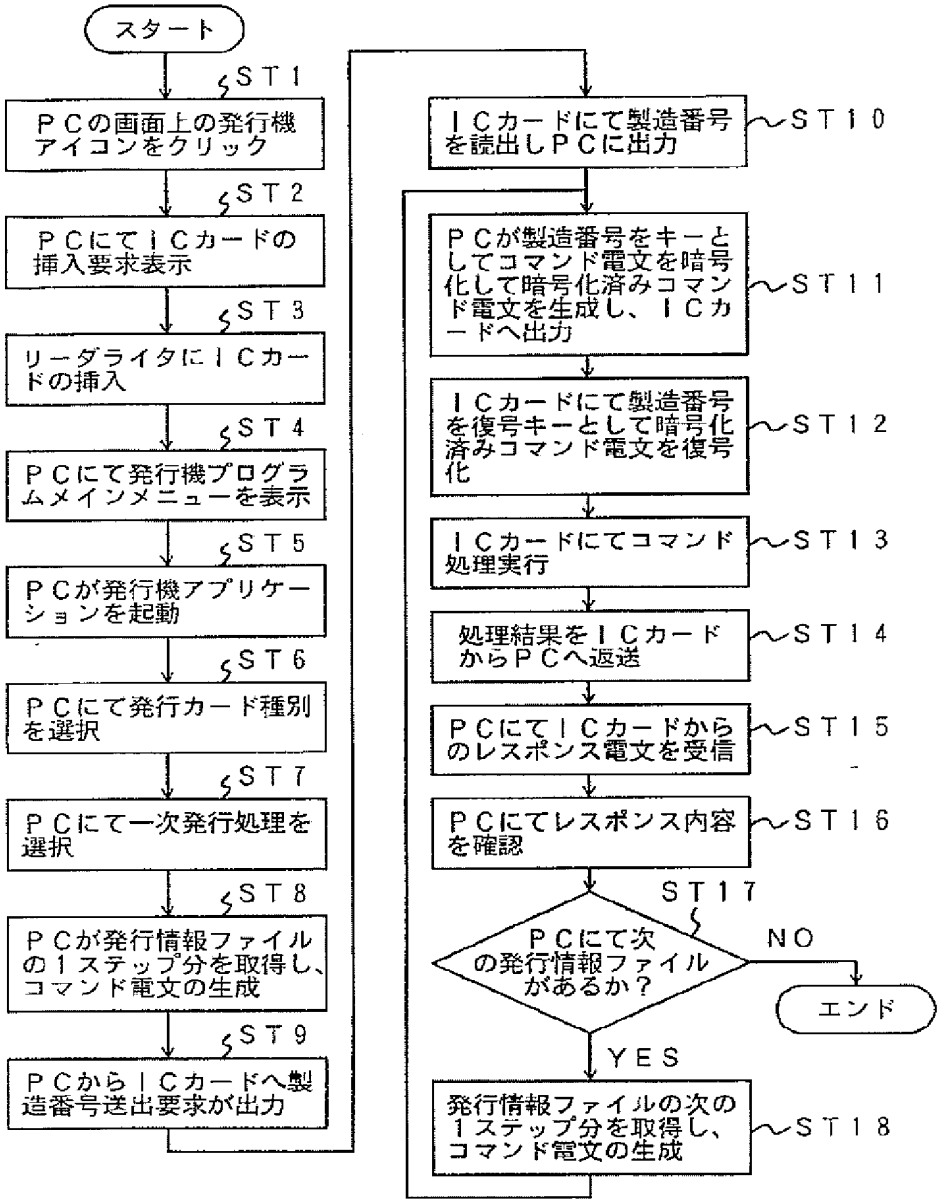
ファイルＩＤ	ファイルサイズ	ファイル種別	参照アクセス権	変更アクセス権

アプリ用データファイル管理情報

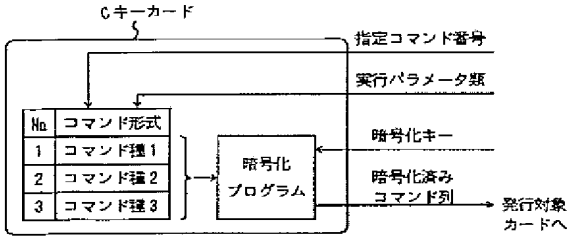
【図２２】



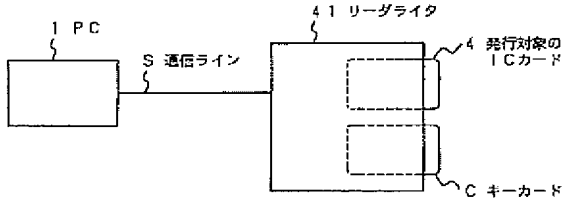
【図１１】


スタート
ＳＴ１
ＰＣの画面上の発行機アイコンをクリック
ＳＴ２
ＰＣにてＩＣカードの挿入要求表示
ＳＴ３
リーダライタにＩＣカードの挿入
ＳＴ４
ＰＣにて発行機プログラムメインメニューを表示
ＳＴ５
ＰＣが発行機アプリケーションを起動
ＳＴ６
ＰＣにて発行カード種別を選択
ＳＴ７
ＰＣにて一次発行処理を選択
ＳＴ８
ＰＣが発行情報ファイルの１ステップ分を取得し、コマンド電文の生成
ＳＴ９
ＰＣからＩＣカードへ製造番号送出要求が出力
ＩＣカードにて製造番号を読出しＰＣに出力
ＳＴ１０
ＰＣが製造番号をキーとしてコマンド電文を暗号化して暗号化済みコマンド電文を生成し、ＩＣカードへ出力
ＳＴ１１
ＩＣカードにて製造番号を復号キーとして暗号化済みコマンド電文を復号化
ＳＴ１２
ＩＣカードにてコマンド処理実行
ＳＴ１３
処理結果をＩＣカードからＰＣへ返送
ＳＴ１４
ＰＣにてＩＣカードからのレスポンス電文を受信
ＳＴ１５
ＰＣにてレスポンス内容を確認
ＳＴ１６
ＳＴ１７
ＰＣにて次の発行情報ファイルがあるか？
ＮＯ
エンド
ＹＥＳ
発行情報ファイルの次の１ステップ分を取得し、コマンド電文の生成
ＳＴ１８

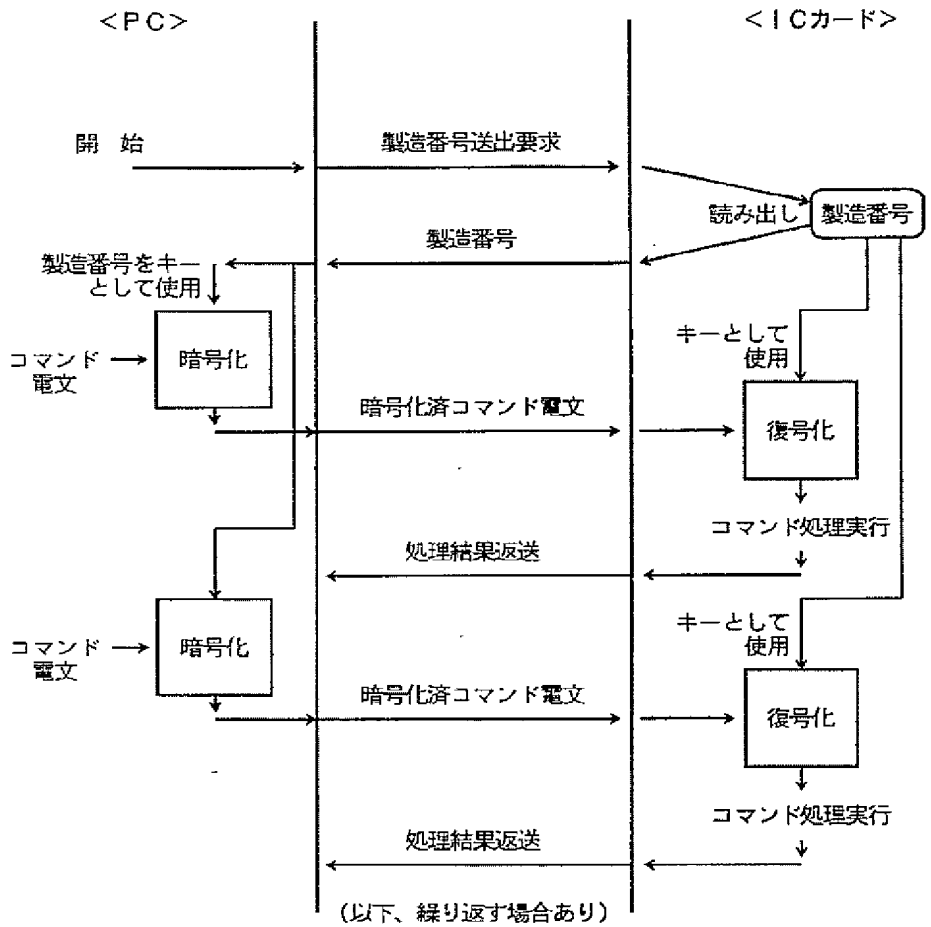
【図２５】


Cキーカード
指定コマンド番号
実行パラメータ類
No
コマンド形式
1
コマンド種1
2
コマンド種2
3
コマンド種3
暗号化プログラム
暗号化キー
暗号化済みコマンド列
発行対象カードへ

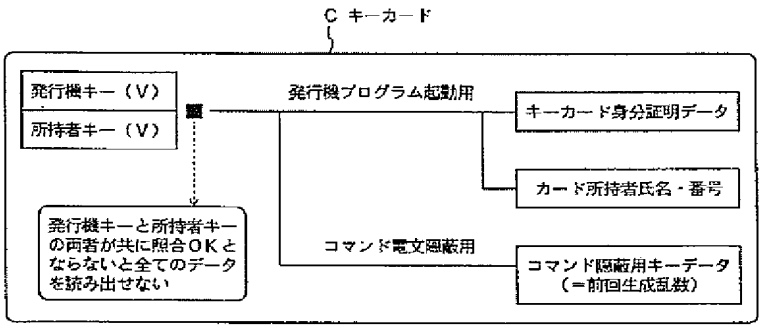
【図２８】


1 PC
S 通信ライン
41 リーダライタ
4 発行対象のICカード
C キーカード

【図１２】



【図２０】

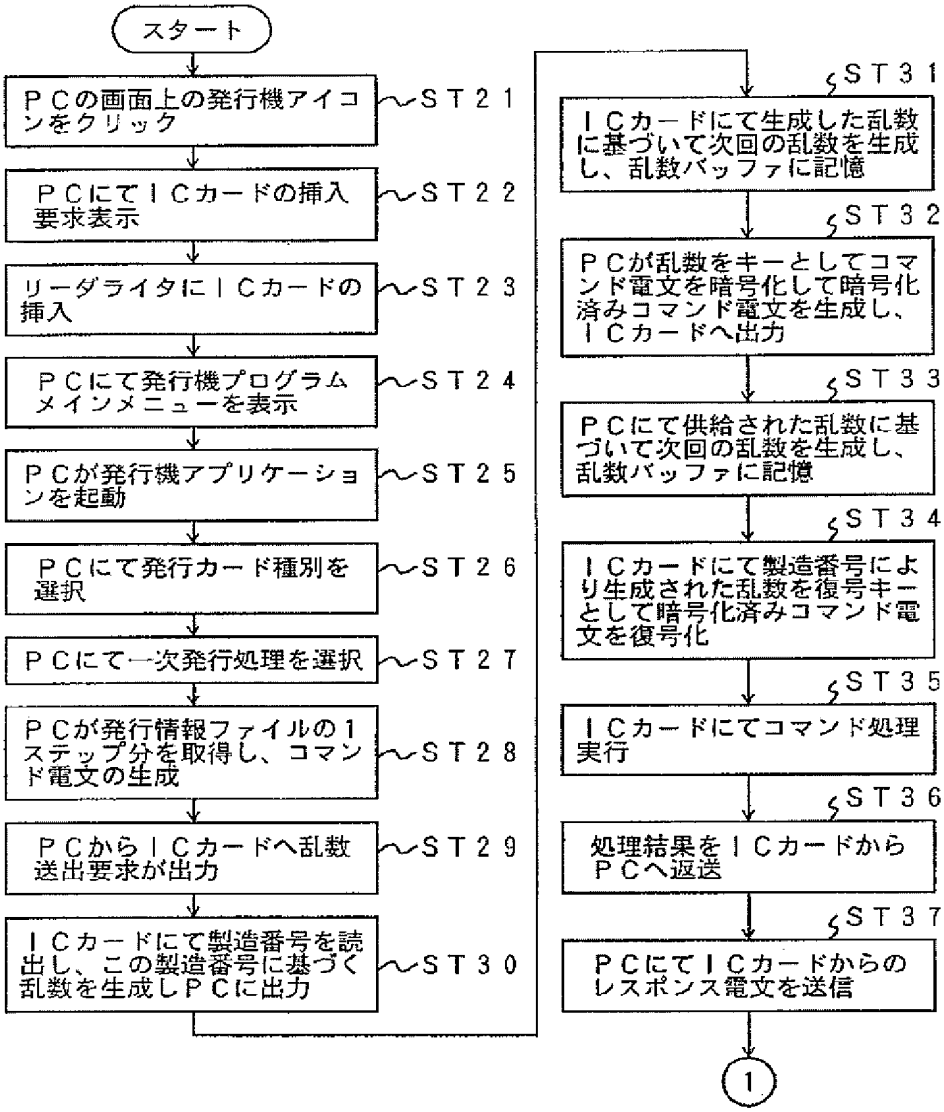


（V）：カード内での照合用データであることを示す

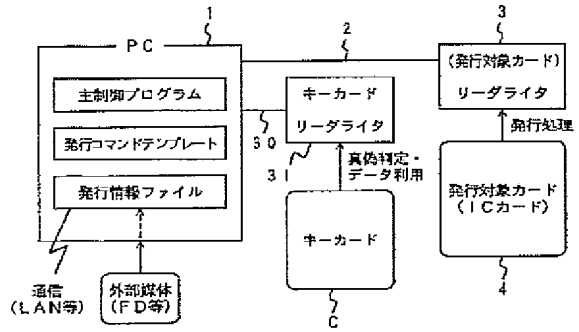
【図３２】

先頭符号	送信電文長	動作種別指示コード	実行パラメータ	処理用データ	末尾符号

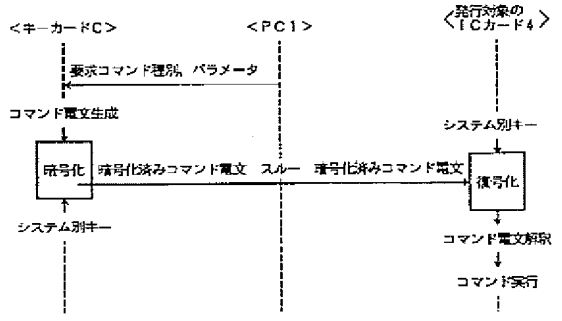
【図１３】


スタート
ＰＣの画面上の発行機アイコンをクリック
ＳＴ２１
ＰＣにてＩＣカードの挿入要求表示
ＳＴ２２
リーダライタにＩＣカードの挿入
ＳＴ２３
ＰＣにて発行機プログラムメインメニューを表示
ＳＴ２４
ＰＣが発行機アプリケーションを起動
ＳＴ２５
ＰＣにて発行カード種別を選択
ＳＴ２６
ＰＣにて一次発行処理を選択
ＳＴ２７
ＰＣが発行情報ファイルの１ステップ分を取得し、コマンド電文の生成
ＳＴ２８
ＰＣからＩＣカードへ乱数送出要求が出力
ＳＴ２９
ＩＣカードにて製造番号を読出し、この製造番号に基づく乱数を生成しＰＣに出力
ＳＴ３０
ＩＣカードにて生成した乱数に基づいて次回の乱数を生成し、乱数バッファに記憶
ＳＴ３１
ＰＣが乱数をキーとしてコマンド電文を暗号化して暗号化済みコマンド電文を生成し、ＩＣカードへ出力
ＳＴ３２
ＰＣにて供給された乱数に基づいて次回の乱数を生成し、乱数バッファに記憶
ＳＴ３３
ＩＣカードにて製造番号により生成された乱数を復号キーとして暗号化済みコマンド電文を復号化
ＳＴ３４
ＩＣカードにてコマンド処理実行
ＳＴ３５
処理結果をＩＣカードからＰＣへ返送
ＳＴ３６
ＰＣにてＩＣカードからのレスポンス電文を送信
ＳＴ３７
①

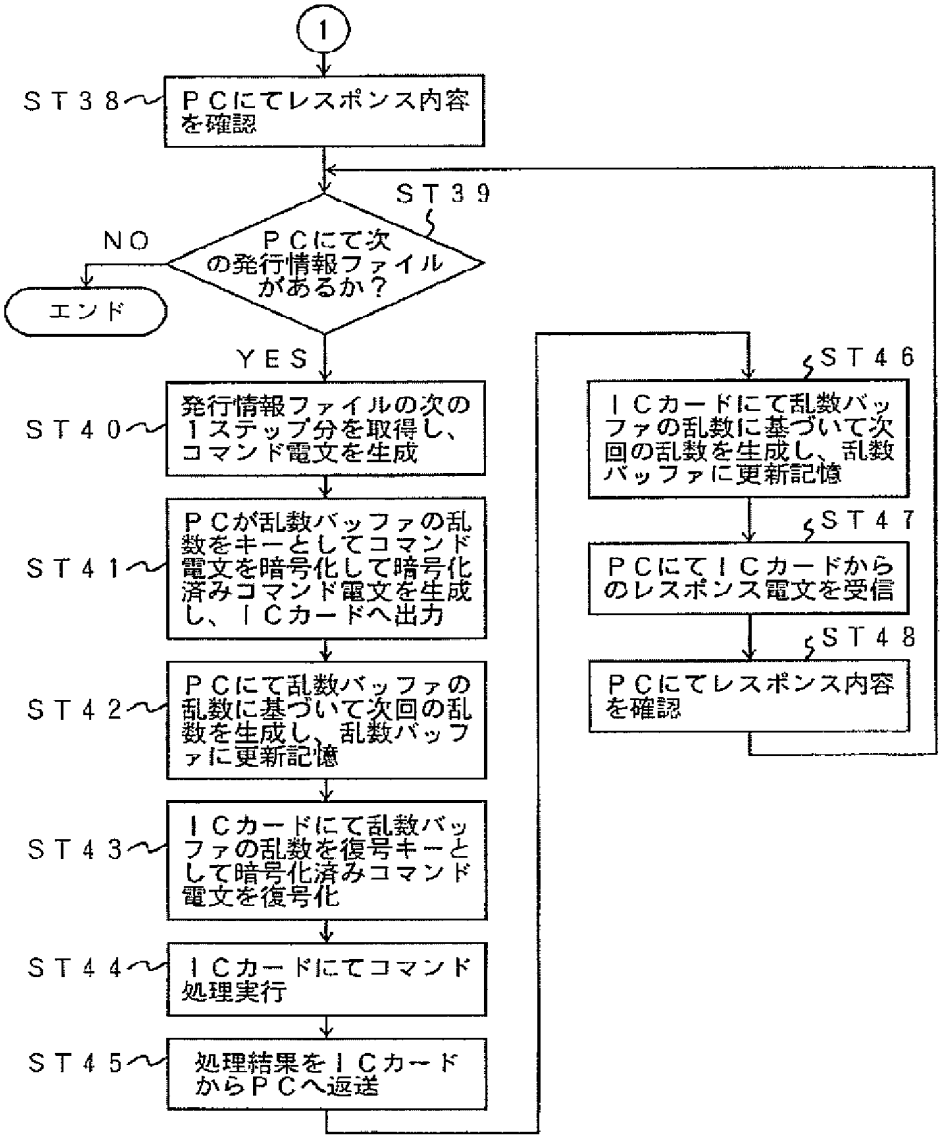
【図２１】


1
PC
主制御プログラム
発行コマンドテンプレート
発行情報ファイル
通信（LAN等）
外部媒体（FD等）
2
キーカード
リーダライタ
30
31
真偽判定・データ利用
キーカード
C
3
（発行対象カード）
リーダライタ
発行処理
発行対象カード（ICカード）
4

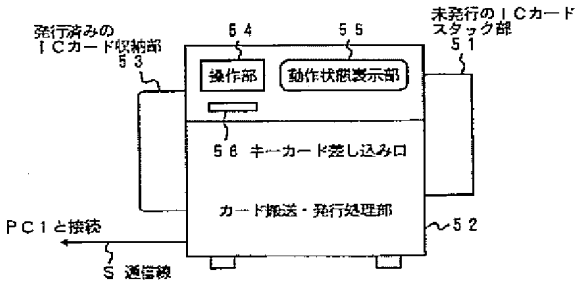
【図２７】


<キーカードC>
<PC1>
<発行対象のICカード4>
要求コマンド種別、パラメータ
コマンド電文生成
システム別キー
暗号化
暗号化済みコマンド電文
スルー
暗号化済みコマンド電文
復号化
システム別キー
コマンド電文解釈
コマンド実行

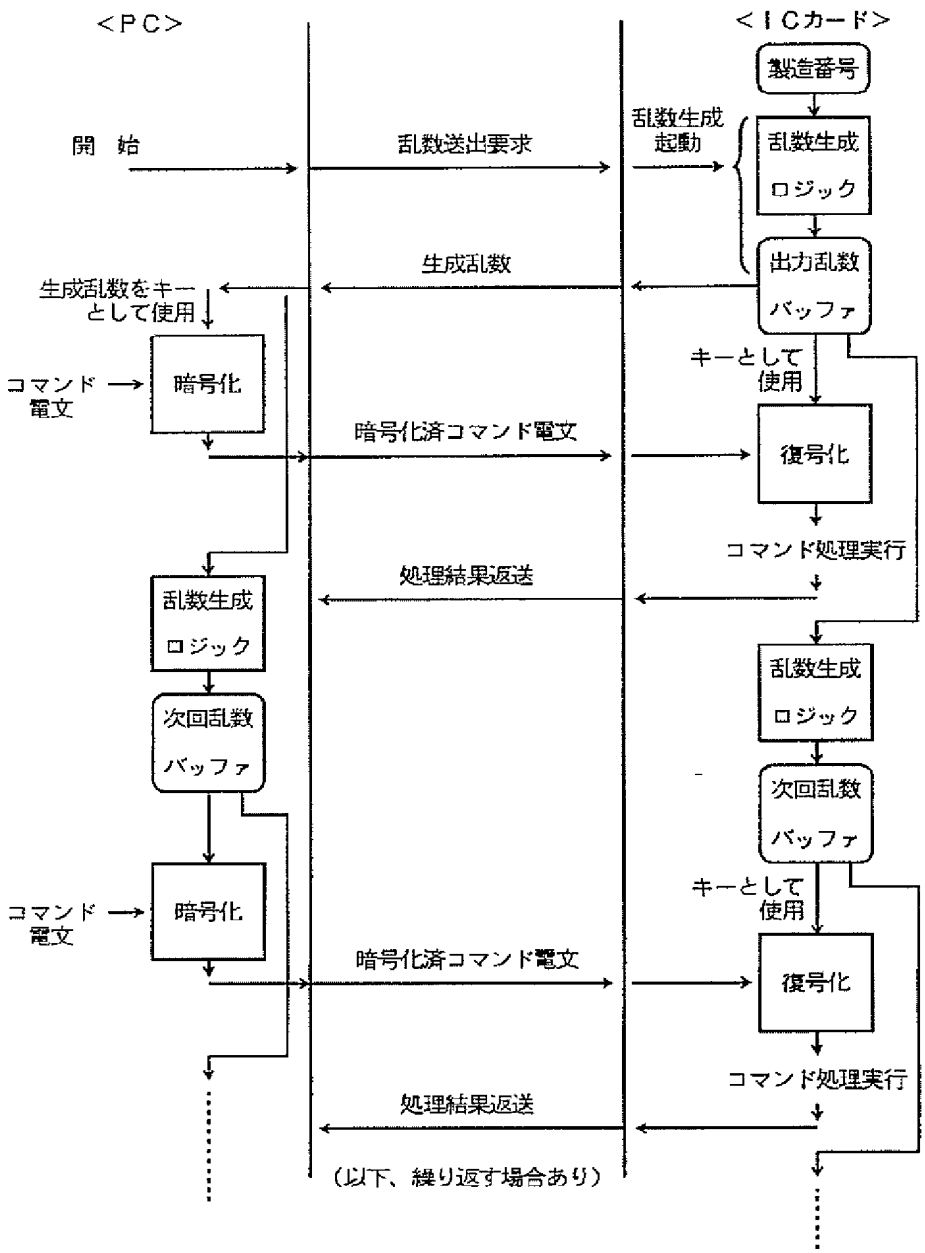
【図１４】


1
ＳＴ３８
ＰＣにてレスポンス内容を確認
ＳＴ３９
ＰＣにて次の発行情報ファイルがあるか？
ＮＯ
エンド
ＹＥＳ
ＳＴ４０
発行情報ファイルの次の１ステップ分を取得し、コマンド電文を生成
ＳＴ４１
ＰＣが乱数バッファの乱数をキーとしてコマンド電文を暗号化して暗号化済みコマンド電文を生成し、ＩＣカードへ出力
ＳＴ４２
ＰＣにて乱数バッファの乱数に基づいて次回の乱数を生成し、乱数バッファに更新記憶
ＳＴ４３
ＩＣカードにて乱数バッファの乱数を復号キーとして暗号化済みコマンド電文を復号化
ＳＴ４４
ＩＣカードにてコマンド処理実行
ＳＴ４５
処理結果をＩＣカードからＰＣへ返送
ＳＴ４６
ＩＣカードにて乱数バッファの乱数に基づいて次回の乱数を生成し、乱数バッファに更新記憶
ＳＴ４７
ＰＣにてＩＣカードからのレスポンス電文を受信
ＳＴ４８
ＰＣにてレスポンス内容を確認

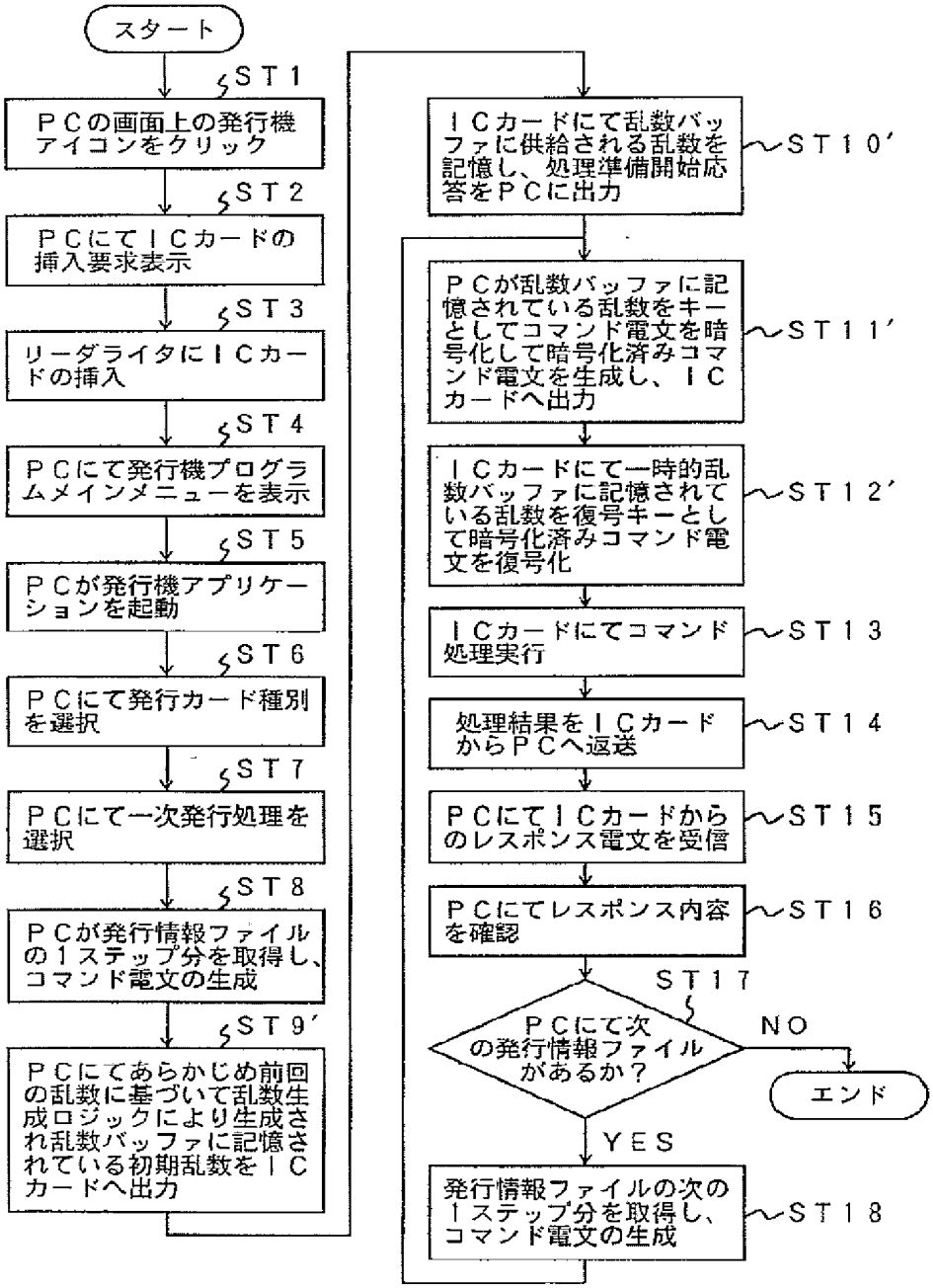
【図２９】


発行済みのＩＣカード収納部
５３
５４
５５
未発行のＩＣカードスタック部
５１
操作部
動作状態表示部
５６ キーカード差し込み口
カード搬送・発行処理部
５２
ＰＣ１と接続
Ｓ 通信線

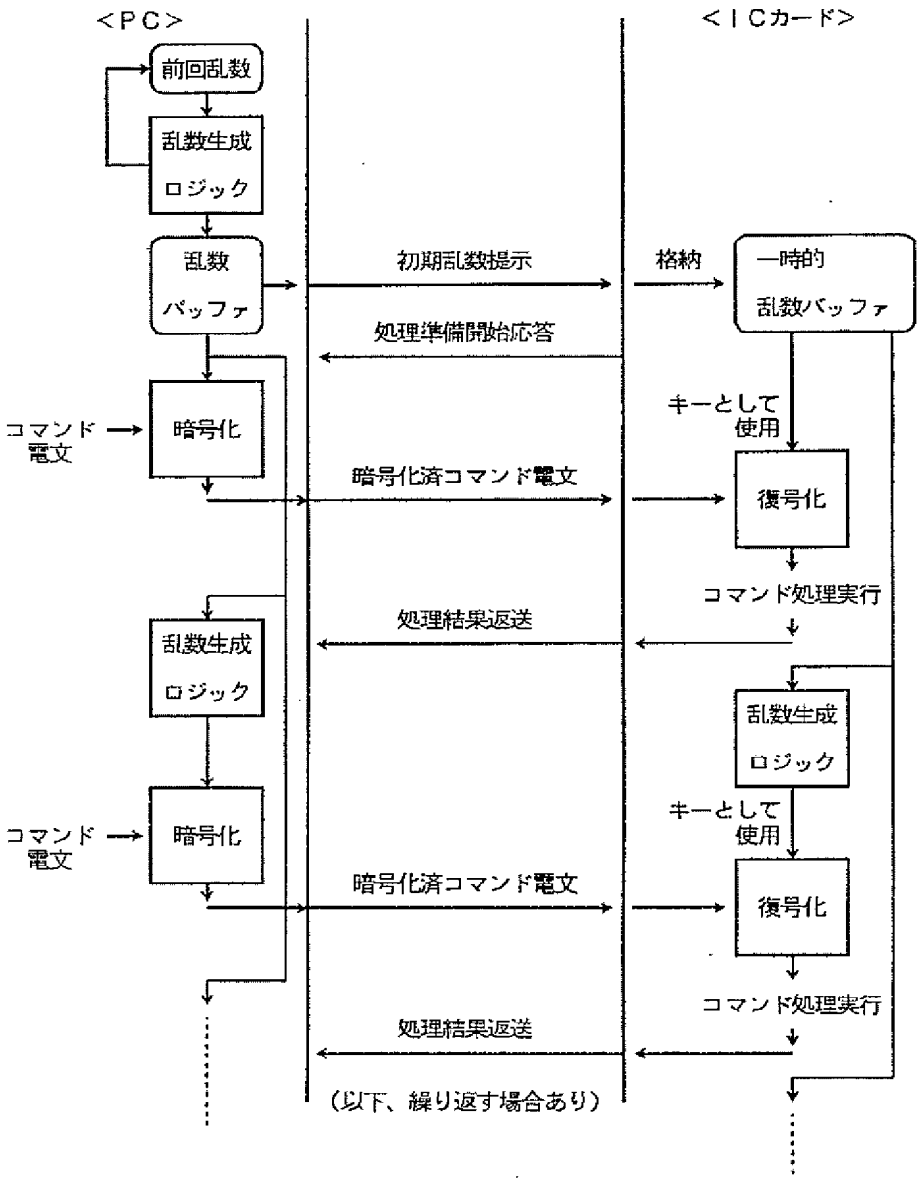
【図１５】


<ＰＣ>
<ＩＣカード>
製造番号
開　始
乱数送出要求
乱数生成
起動
乱数生成
ロジック
出力乱数
バッファ
生成乱数
生成乱数をキー
として使用
キーとして
使用
コマンド
電文
暗号化
暗号化済コマンド電文
復号化
コマンド処理実行
処理結果返送
乱数生成
ロジック
次回乱数
バッファ
乱数生成
ロジック
次回乱数
バッファ
キーとして
使用
コマンド
電文
暗号化
暗号化済コマンド電文
復号化
コマンド処理実行
処理結果返送
（以下、繰り返す場合あり）

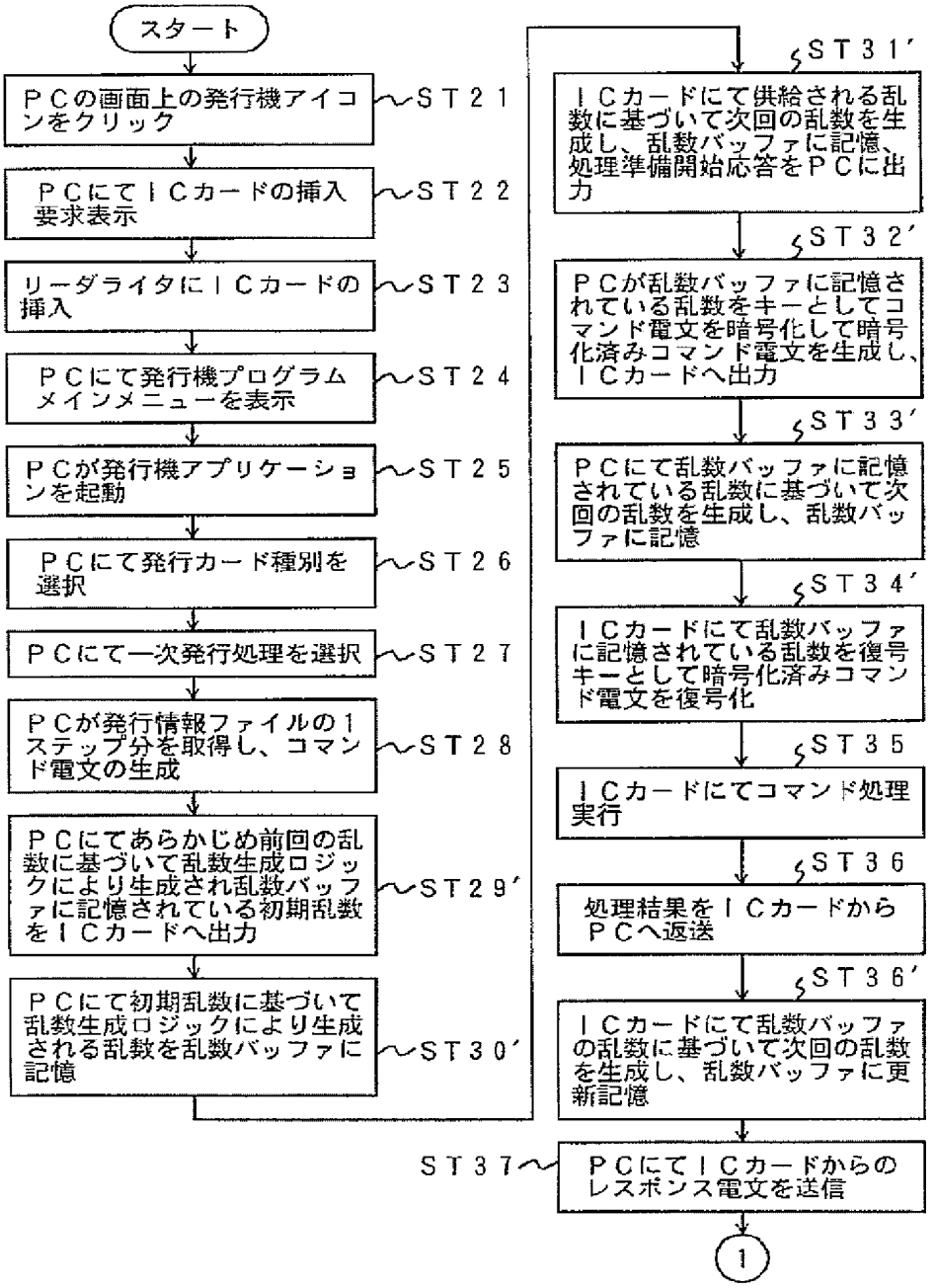
【図１６】


スタート
ＳＴ１
ＰＣの画面上の発行機アイコンをクリック
ＳＴ２
ＰＣにてＩＣカードの挿入要求表示
ＳＴ３
リーダライタにＩＣカードの挿入
ＳＴ４
ＰＣにて発行機プログラムメインメニューを表示
ＳＴ５
ＰＣが発行機アプリケーションを起動
ＳＴ６
ＰＣにて発行カード種別を選択
ＳＴ７
ＰＣにて一次発行処理を選択
ＳＴ８
ＰＣが発行情報ファイルの１ステップ分を取得し、コマンド電文の生成
ＳＴ９′
ＰＣにてあらかじめ前回の乱数に基づいて乱数生成ロジックにより生成され乱数バッファに記憶されている初期乱数をＩＣカードへ出力
ＩＣカードにて乱数バッファに供給される乱数を記憶し、処理準備開始応答をＰＣに出力
ＳＴ１０′
ＰＣが乱数バッファに記憶されている乱数をキーとしてコマンド電文を暗号化して暗号化済みコマンド電文を生成し、ＩＣカードへ出力
ＳＴ１１′
ＩＣカードにて一時的乱数バッファに記憶されている乱数を復号キーとして暗号化済みコマンド電文を復号化
ＳＴ１２′
ＩＣカードにてコマンド処理実行
ＳＴ１３
処理結果をＩＣカードからＰＣへ返送
ＳＴ１４
ＰＣにてＩＣカードからのレスポンス電文を受信
ＳＴ１５
ＰＣにてレスポンス内容を確認
ＳＴ１６
ＳＴ１７
ＰＣにて次の発行情報ファイルがあるか？
ＮＯ
エンド
ＹＥＳ
発行情報ファイルの次の１ステップ分を取得し、コマンド電文の生成
ＳＴ１８

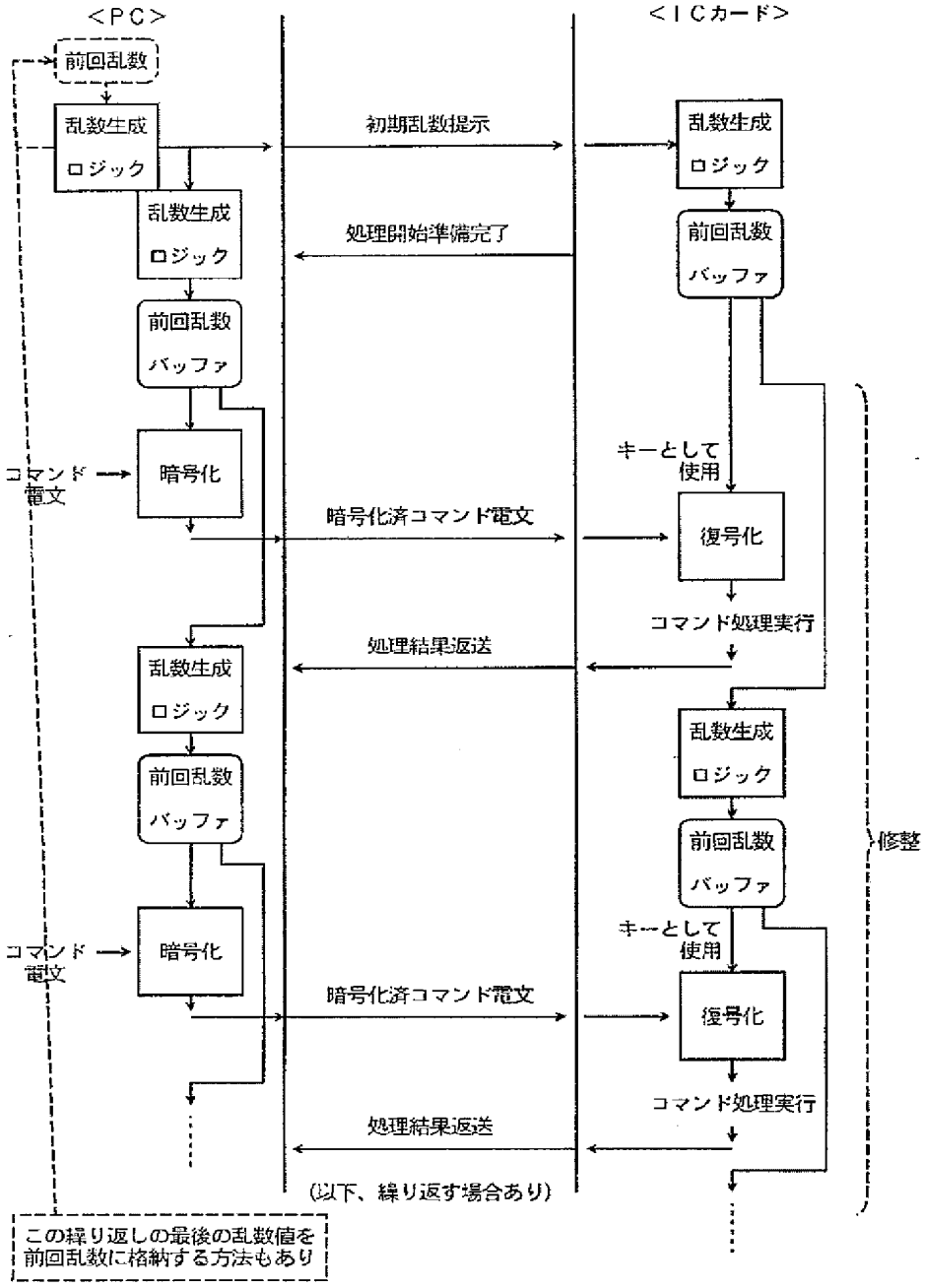
【図１７】


<ＰＣ>
<ＩＣカード>
前回乱数
乱数生成ロジック
乱数バッファ
初期乱数提示
格納
一時的乱数バッファ
処理準備開始応答
コマンド電文
暗号化
キーとして使用
暗号化済コマンド電文
復号化
コマンド処理実行
処理結果返送
乱数生成ロジック
コマンド電文
暗号化
キーとして使用
暗号化済コマンド電文
復号化
コマンド処理実行
処理結果返送
（以下、繰り返す場合あり）

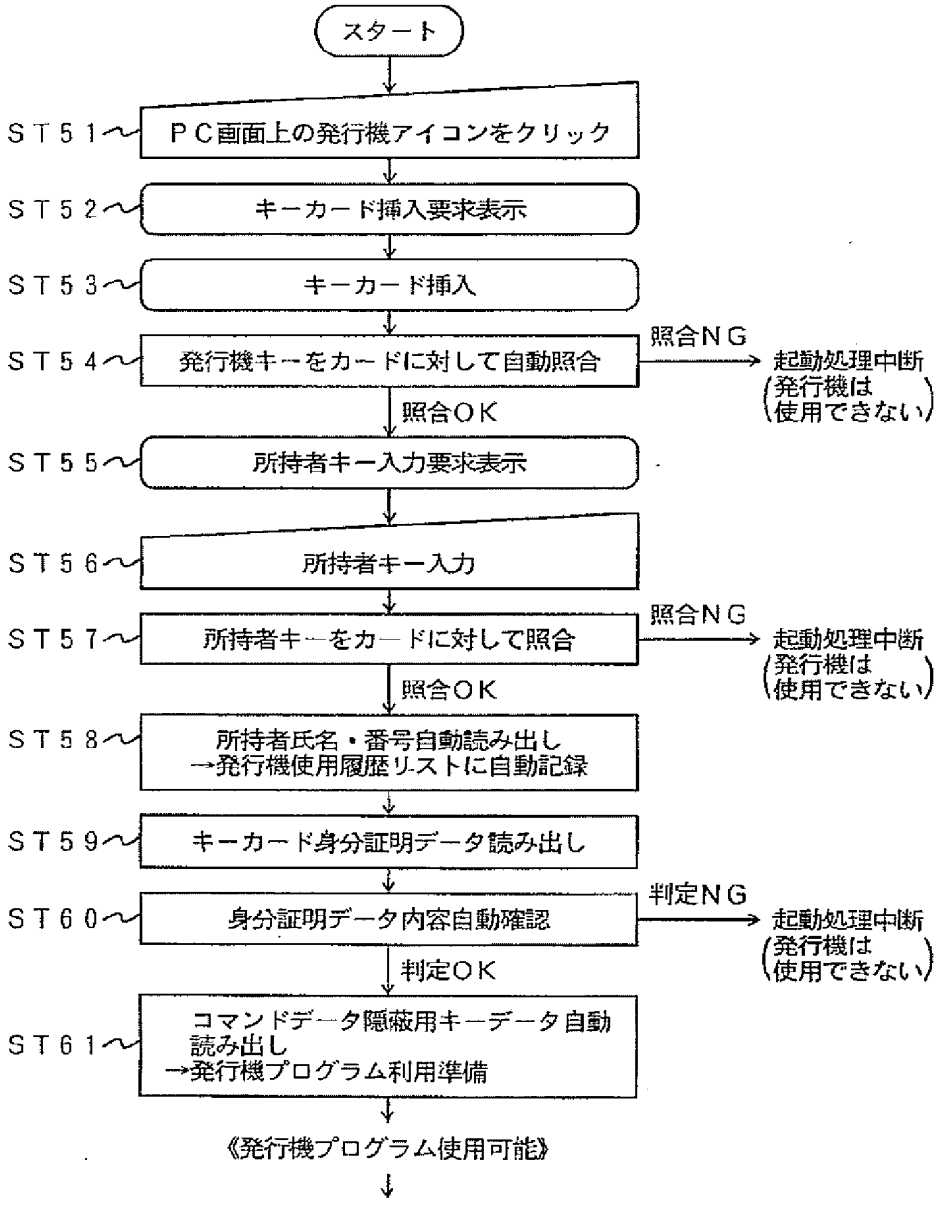
【図１８】


スタート
ＰＣの画面上の発行機アイコンをクリック
ＳＴ２１
ＰＣにてＩＣカードの挿入要求表示
ＳＴ２２
リーダライタにＩＣカードの挿入
ＳＴ２３
ＰＣにて発行機プログラムメインメニューを表示
ＳＴ２４
ＰＣが発行機アプリケーションを起動
ＳＴ２５
ＰＣにて発行カード種別を選択
ＳＴ２６
ＰＣにて一次発行処理を選択
ＳＴ２７
ＰＣが発行情報ファイルの１ステップ分を取得し、コマンド電文の生成
ＳＴ２８
ＰＣにてあらかじめ前回の乱数に基づいて乱数生成ロジックにより生成され乱数バッファに記憶されている初期乱数をＩＣカードへ出力
ＳＴ２９′
ＰＣにて初期乱数に基づいて乱数生成ロジックにより生成される乱数を乱数バッファに記憶
ＳＴ３０′
ＳＴ３１′
ＩＣカードにて供給される乱数に基づいて次回の乱数を生成し、乱数バッファに記憶、処理準備開始応答をＰＣに出力
ＳＴ３２′
ＰＣが乱数バッファに記憶されている乱数をキーとしてコマンド電文を暗号化して暗号化済みコマンド電文を生成し、ＩＣカードへ出力
ＳＴ３３′
ＰＣにて乱数バッファに記憶されている乱数に基づいて次回の乱数を生成し、乱数バッファに記憶
ＳＴ３４′
ＩＣカードにて乱数バッファに記憶されている乱数を復号キーとして暗号化済みコマンド電文を復号化
ＳＴ３５
ＩＣカードにてコマンド処理実行
ＳＴ３６
処理結果をＩＣカードからＰＣへ返送
ＳＴ３６′
ＩＣカードにて乱数バッファの乱数に基づいて次回の乱数を生成し、乱数バッファに更新記憶
ＳＴ３７
ＰＣにてＩＣカードからのレスポンス電文を送信
1

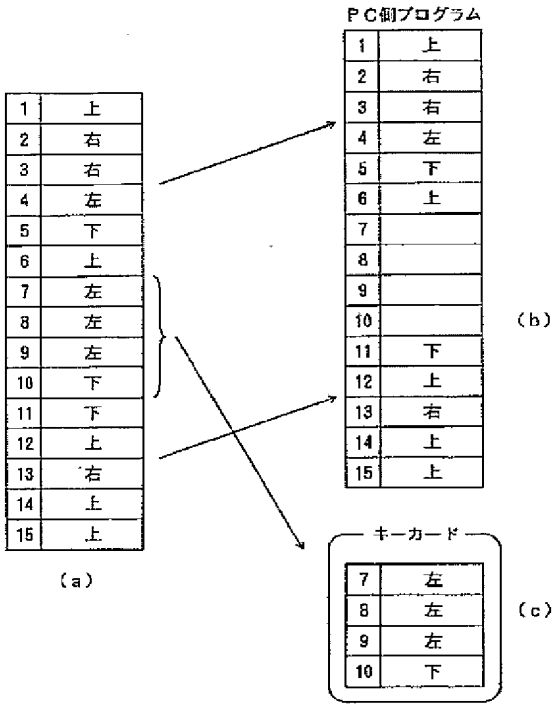
【図１９】


<PC>
<ICカード>
前回乱数
乱数生成ロジック
初期乱数提示
乱数生成ロジック
乱数生成ロジック
処理開始準備完了
前回乱数バッファ
前回乱数バッファ
キーとして使用
コマンド電文
暗号化
暗号化済コマンド電文
復号化
コマンド処理実行
処理結果返送
乱数生成ロジック
前回乱数バッファ
乱数生成ロジック
前回乱数バッファ
修整
キーとして使用
コマンド電文
暗号化
暗号化済コマンド電文
復号化
コマンド処理実行
処理結果返送
(以下、繰り返す場合あり)
この繰り返しの最後の乱数値を前回乱数に格納する方法もあり

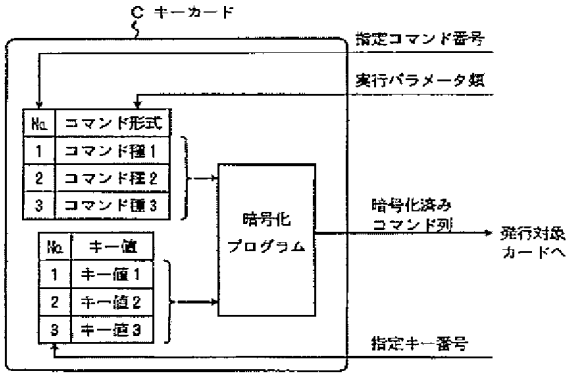
【図２３】


スタート
ＳＴ５１
ＰＣ画面上の発行機アイコンをクリック
ＳＴ５２
キーカード挿入要求表示
ＳＴ５３
キーカード挿入
ＳＴ５４
発行機キーをカードに対して自動照合
照合ＮＧ
起動処理中断
(発行機は
使用できない)
照合ＯＫ
ＳＴ５５
所持者キー入力要求表示
ＳＴ５６
所持者キー入力
ＳＴ５７
所持者キーをカードに対して照合
照合ＮＧ
起動処理中断
(発行機は
使用できない)
照合ＯＫ
ＳＴ５８
所持者氏名・番号自動読み出し
→発行機使用履歴リストに自動記録
ＳＴ５９
キーカード身分証明データ読み出し
ＳＴ６０
身分証明データ内容自動確認
判定ＮＧ
起動処理中断
(発行機は
使用できない)
判定ＯＫ
ＳＴ６１
コマンドデータ隠蔽用キーデータ自動
読み出し
→発行機プログラム利用準備
《発行機プログラム使用可能》

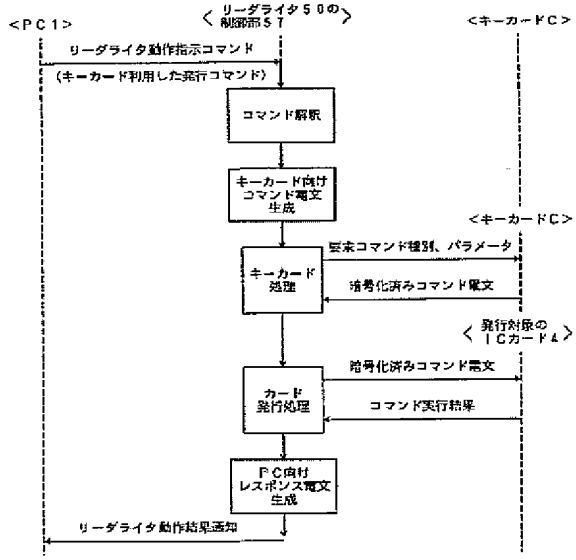
【図２４】



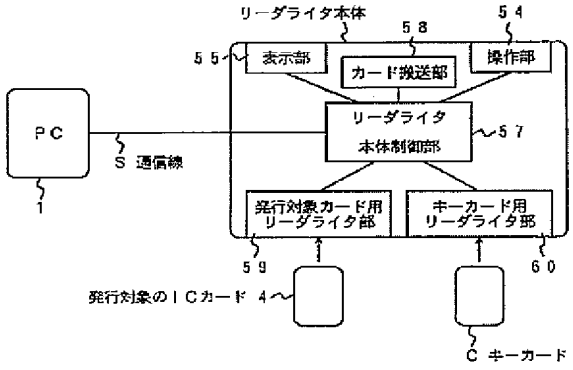
【図２６】



【図３１】



【図３０】



フロントページの続き

(51) Int.Cl.[7]	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
H04L 9/36		H04L 9/00	685